

Classical simulation of measurement-based quantum computation on higher-genus surface-code states

Leonard Goff and Robert Raussendorf

Department of Physics and Astronomy, University of British Columbia, Vancouver, British Columbia V6T 1Z1, Canada

(Dated: November 1, 2012)

We consider the efficiency of classically simulating measurement-based quantum computation on surface-code states. We devise a method for calculating the elements of the probability distribution for the classical output of the quantum computation. The operational cost of this method is polynomial in the size of the surface-code state, but in the worst case scales as 2^{2g} in the genus g of the surface embedding the code. However, there are states in the code space for which the simulation becomes efficient. In general, the simulation cost is exponential in the entanglement contained in a certain effective state, capturing the encoded state, the encoding and the local post-measurement states. The same efficiencies hold, with additional assumptions on the temporal order of measurements and on the tessellations of the code surfaces, for the harder task of sampling from the distribution of the computational output.

I. INTRODUCTION

A major open problem in quantum computation is to determine the physical properties of quantum systems that account for the quantum speedup over classical computation. This would aid in the development of useful quantum computational systems, and constitute a significant leap forward in our understanding of quantum physics.

One approach to studying this problem is to find instances of quantum computational processes that can be simulated efficiently on a classical computer, and identify which quantum mechanical properties they lack. There are three known examples in this category; namely quantum circuits composed of Clifford gates [1], matchgate circuits [2], [3] (which can be mapped to non-interacting fermions [4]), and quantum evolutions in which the entanglement—as quantified by an appropriate monotone—always remains small [5], [6].

Specifically, it was shown in [5] that any circuit model quantum computation can be classically simulated with a number of steps that grows polynomially in the number of qubits, but exponentially in an entanglement measure χ . Therein, χ is the log of the maximum value of the Schmidt rank across any bipartition of the set of qubits, at any point of the computation. This result has counterparts in measurement-based quantum computation (MBQC) [7], [8]. However, such results relating the amount of entanglement present in a quantum system to the hardness of its classical simulation need to be taken with a grain of salt: they do not hold for all entanglement measures. Specifically, they do not hold for sufficiently continuous entanglement measures [9]. Also note that quantum states can be too entangled to be useful for MBQC [10], [11].

In this paper we describe a classical simulation method for quantum systems that combines the fermionic or matchgate method with that for slightly entangled quantum systems. To this end, we consider the classical simulation of MBQC where the initial resource state is a state

in the code space of the surface code. The originally intended application for surface codes is fault-tolerant quantum computation in two-dimensional local architectures with constrained interaction range [12], [13]. Regarding the potential use of surface-code states as resources in MBQC, it was previously shown that for such states with a planar topology the resulting quantum computation can be efficiently classically simulated [14], [15].

Here, we extend this investigation to surface-codes embedded in surfaces of higher genus. This problem is related to, but not the same as matchgate contraction [16] and computing the Ising model partition function [17] on higher genus graphs. We focus initially on the computation of the probability of obtaining any single sequence of MBQC measurement outcomes, starting from a surface-code state. Our results are that: (1) In the worst case this can be done with a cost that scales polynomially in the size of the resource, but exponentially in the genus. (2) For any genus g the code space has a basis such that for each basis state the computation is efficient, and (3) There exists an effective state $|\Phi\rangle$ constructed out of the code, the encoded state and the post-measurement unentangled state such that the cost of classically simulating MBQC is exponential in the entanglement of $|\Phi\rangle$. By specializing to a specific family of higher genus graphs and ordering of measurements, we are able to extend these efficiencies to the harder task of sampling from the probability distribution over MBQC outcomes.

The remainder of this paper is organized as follows. In Section II, we define the surface code on tessellations of surfaces of genus g . In Section III, we introduce the notions of classical simulation to be used in this paper. In Section IV, we present a method for pointwise evaluating the output distribution of MBQC. In Section V we discuss the efficiency of evaluating partial measurement probabilities, in order to efficiently sample from the output distribution. We conclude in Section VI.

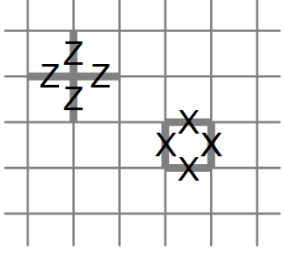


FIG. 1: The stabilizer group of the surface code is generated by an X-type operator around the boundary of every face, and a Z-type operator on the set of edges incident on every vertex.

II. THE SURFACE CODE

A. Definition

To define the surface code, we first introduce the notion of a graph embedded on a surface. See [18] for a detailed introduction. In this paper, we consider closed, orientable surfaces S of genus g . Given a graph $G = (V, E)$, we say that G is *embedded on S* when G is drawn on S with no edge crossings. The surface S (minus the image of the embedding) is partitioned by the graph into disjoint regions called *faces*, which are separated from one another by the curves representing edges of G . The set of faces is denoted as F , and for any $f \in F$, ∂f denotes the *boundary* of f , which is the set of edges which separate f from other faces. For any vertex $v \in V$, we let δv denote the set of edges that are incident upon v in G . We consider here so-called *cellular embeddings*, which have the property that each face is homeomorphic to an open disk. For a graph G cellularly embedded on a closed, orientable surface of genus g , Euler's formula holds: $|E| - |V| - |F| = 2 - 2g$. When using the term *graph*, we allow for self-loops and redundant edges (what some authors call a *multigraph*), unless explicitly stated otherwise.

Consider a graph G cellularly embedded on an orientable surface S : $G = (V, E, F)$, where G is connected. We associate a qubit with each edge $e \in E$. The surface code is a stabilizer code with stabilizer generators[19]:

$$A_v := \prod_{e \in \delta v} Z_e \quad \forall v \in V,$$

$$B_f := \prod_{e \in \partial f} X_e \quad \forall f \in F.$$

The code space \mathcal{CS} is defined as the joint $+1$ eigenspace of all of the stabilizer generators

$$\mathcal{CS} := \{|\psi\rangle : A_v|\psi\rangle = B_f|\psi\rangle = |\psi\rangle \quad \forall v \in V, f \in F\}.$$

The stabilizers all commute, because for any $v \in V$ and $f \in F$, δv and ∂f always have an even number of edges in common. If G contains any self-loops, then the

corresponding edge qubit will be disentangled from the rest for any state $|\psi\rangle \in \mathcal{CS}$, and in the $+1$ X eigenstate. We neglect any such qubit and assume that G contains no self-loops.

For each of the two types of stabilizer generator, any single one can be written as a product of all of the others. Thus, there are $|V| + |F| - 2$ independent, commuting stabilizer generators. It follows from Euler's formula and the theory of stabilizer codes [20] that the dimensionality of \mathcal{CS} is 2^{2g} , so the surface code allows for the encoding of $2g$ logical qubits.

B. Encoded Pauli operators

We now seek $2g$ encoded Pauli X operators \bar{X}_j and encoded Pauli Z operators \bar{Z}_j for $j = 1 \dots 2g$. To do so, we shall introduce a few more notions from topological graph theory. A *cycle* C is a set of edges such that every vertex has an even number of edges incident upon it from C [21]. The symmetric difference of any two cycles C_1 and C_2 is also a cycle, which we shall refer to as the *sum* of C_1 and C_2 . A cycle is called *trivial* if it can be obtained as the sum of the boundaries of some set of faces. Two cycles are called *homologous* on G if their sum is a trivial cycle. This equivalence relation divides the set of all cycles on G into *homology classes* of mutually homologous cycles. The set of homology classes forms a group under addition, called the first homology group. Each handle in a surface S contributes two independent generators to the first homology group, which is isomorphic to \mathbb{Z}^{2g} . Intuitively, the two generators can be thought of as the cycles that go around the handle, and the cycles that go through it.

An operator of the form $\bar{X} = \prod_{e \in C} X_e$ for any cycle C will commute with all of the stabilizer generators of the surface code. If C is a trivial cycle, then \bar{X} is equal to a product of some set of B_f operators, and thus acts trivially on the code space. With this in mind, we define the encoded X operators as $\bar{X}_j = \prod_{e \in C_j} X_e$, where $\{C_j\}$ is a set of $2g$ nontrivial cycles, which are *homologically independent*. By homologically independent, we mean that no non-trivial linear combination of the cycles $\{C_j\}$ is homologically trivial. This ensures that the \bar{X}_j all act independently on \mathcal{CS} while commuting with the stabilizer generators.

To define the encoded Pauli Z operators, we use the same construction, but on the dual graph. For an embedded graph $G = (V, E, F)$, its *dual graph* \tilde{G} swaps the roles of vertices and faces. That is, for each face in the original graph we associate a vertex of the dual graph. Two vertices in \tilde{G} are then connected by an edge iff the associated faces of G share an edge. If an edge $e \in E$ is contained entirely within a single face of G , rather than separating two distinct faces, then we draw a self-loop in \tilde{G} for e . A cycle C' on \tilde{G} is called a *cocycle* on G , and has the property that $C' \subseteq E : |C' \cap \partial f| = 0 \pmod{2} \forall f \in F$. The

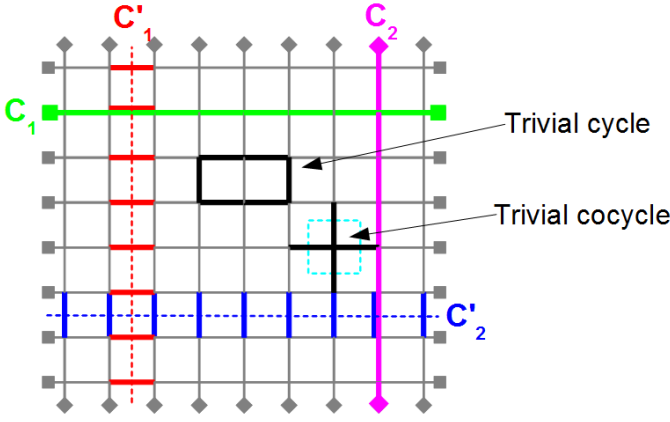


FIG. 2: (Color online) A square toroidal graph ($g = 1$), depicted on a plane. The torus is reconstructed by identifying the points marked with diamonds, as well as the points marked with squares. See text for definitions of the cycles and cocycles shown.

dual of an embedded graph has a natural embedding on the same surface S as the original graph, where we place each vertex of \tilde{G} in the center of the associated face of G [18]. Thus, there are also 2^{2g} distinct homology classes of cocycles on G , where homology is defined with respect to the dual graph embedding. A cocycle on G is trivial if it can be written as $\bigoplus_{v \in \bar{V}} \delta_v$ for some set of vertices $\bar{V} \subseteq V$. We define the encoded Pauli Z operators as $\bar{Z}_j = \prod_{e \in C'_j} Z_e$, where $\{C'_j\}$ is a set of $2g$ homologically independent nontrivial cocycles. To ensure that each encoded X operator anticommutes with the encoded Z operator for the same logical qubit, but commutes with the Z operator for other logical qubits, we must choose the C_j and C'_j such that $|C_j \cap C'_k| = \delta_{jk} \pmod{2}$. Figure 2 depicts such a choice of “encoding cycles” and cocycles for a square toroidal graph.

An algorithm to find a suitable set of cycles C_k and cocycles C'_k satisfying the above criteria - as well as a guarantee of their existence - is provided by the notion of a *tree-cotree decomposition* for an embedded graph, introduced by Eppstein [22]. For any connected graph G , there exists at least one *spanning tree* of G , which is defined as a subset of E that forms a tree (is connected and contains no non-null cycles) and visits every vertex in V . A spanning tree $T \subseteq E$ contains $|V| - 1$ edges. For any spanning tree T , there exists at least one set of edges C within the complement $E \setminus T$ of T in E such that C is a spanning *cotree* of G : that is, a spanning tree of the dual graph \tilde{G} . A spanning cotree contains $|F| - 1$ edges. For a cellularly embedded graph G , Euler’s formula implies that the set of leftover edges $X = E \setminus (T \cup C)$ has a cardinality of $2g$. For each edge $e \in X$, the subgraph with edges $T \cup e$ contains exactly one cycle, which we will denote as $T(e)$. Similarly, $C \cup e$ contains exactly one cocycle $C(e)$. If we label the edges in X arbitrarily as $X = \{e_1 \dots e_{2g}\}$ and define $C_j := T(e_j)$ and $C'_j := C(e_j)$,

then $C_j \cap C'_j = \{e_j\}$ and $C_j \cap C'_k = \emptyset$ for $k \neq j$. The cycles $T(X)$ are also homologically independent (and by corollary likewise for the cocycles $C(X)$) [23]. Thus, a tree-cotree decomposition always provides a suitable definition for the encoded operators of the surface code.

C. The surface-code space

Now that we have defined encoded qubit operators, we can explicitly construct their eigenstates from the eigenstates of the physical Pauli Z operators. Let $|x\rangle = |x_1 \dots x_{|E|}\rangle$ for any $|E|$ component bitstring x be an eigenstate of the physical Z operators, with eigenvalue $(-1)^{x_e}$ for the operator Z_e . The unique mutual $+1$ eigenstate of the $2g$ encoded Pauli X operators is

$$|\bar{+}\rangle = |K(G)\rangle := \frac{1}{\sqrt{|E_0(G)|}} \sum_{x \in E_0(G)} |x\rangle, \quad (1)$$

where $E_0(G)$ is the set of bitstrings corresponding to all cycles on G . We associate bitstrings over E and subsets of E in the natural way: $x_e = 1$ iff e is in the subset. That the state $|\bar{+}\rangle$ is stabilized by all of the A_v operators follows from the fact that since x is a cycle, $A_v|x\rangle = (-1)^{|x \cap \delta_v|}|x\rangle = |x\rangle$. $|\bar{+}\rangle$ is stabilized by all of the B_f operators, because $B_f|x\rangle = |x \oplus \partial f\rangle$, where \oplus denotes mod 2 addition of bitstrings (or equivalently, the symmetric difference of the associated sets). Since $x \oplus \partial f$ is also a cycle and bitwise addition is invertible, operating on $|\bar{+}\rangle$ by B_f merely permutes the order of the symmetric summation over $E_0(G)$ in Equation 1. For this same reason, $\bar{X}_j|\bar{+}\rangle = |\bar{+}\rangle$ for all $j = 1 \dots 2g$.

From the state $|\bar{+}\rangle$, we can construct the rest of the encoded X eigenbasis for \mathcal{CS} by selective application of encoded Z operators. Letting α be any $2g$ component bitstring $\alpha_1 \dots \alpha_{2g}$, the state

$$|\bar{X}_\alpha\rangle := \left(\prod_{j=1}^{2g} \bar{Z}_j^{\alpha_j} \right) |\bar{+}\rangle \quad (2)$$

is the encoded Pauli X eigenstate with eigenvalue $(-1)^{\alpha_j}$ for \bar{X}_j . The states $|\bar{X}_\alpha\rangle$ provide an orthonormal basis for \mathcal{CS} , because

$$\langle \bar{X}_\gamma | \bar{X}_\alpha \rangle = \langle \bar{+} | \left(\prod_{j=1}^{2g} (\bar{Z}_j)^{\alpha_j \oplus \gamma_j} \right) |\bar{+}\rangle.$$

If $\gamma_j \neq \alpha_j$ for any j , then one can prove that $\langle \bar{X}_\gamma | \bar{X}_\alpha \rangle = -\langle \bar{X}_\gamma | \bar{X}_\alpha \rangle = 0$ by inserting an \bar{X}_j operator into the above expression and anticommuting it past \bar{Z}_j . If on the other hand $\gamma_j = \alpha_j$ for all j , then $\langle \bar{X}_\gamma | \bar{X}_\alpha \rangle = \langle \bar{+} | \bar{+} \rangle = 1$ as expected.

The set $E_0(G)$ appearing in Equation 1 is the so-called *cycle space* of G . From the definition of a cycle and Euler’s formula, one can determine the size of the cycle

space to be $|E_0(G)| = 2^{|E|-|V|+1} = 2^{2g+|F|-1}$, assuming that G is connected (see Section V A for proof). The cycle space of G is a vector space over the binary field \mathbb{Z}_2 with a basis composed of all of the face boundaries except one, as well as any set of $2g$ homologically independent nontrivial cycles (such as the C_j).

III. CLASSICAL SIMULATION OF MBQC ON SURFACE-CODE STATES

In this section, we define our notions of classical simulation of MBQC. A run of MBQC begins with putting in place a resource state $|\mathcal{R}\rangle$, which in the context of the present paper is a state in the code space of a surface code. Subsequently, all qubits in the support of $|\mathcal{R}\rangle$ are measured, where measurement bases are possibly adapted depending on the outcomes of earlier measurements. Finally, the classical output bits, collectively denoted by the vector \mathbf{o} , are computed as certain parities among measurement outcomes. The probability distribution for the various values of the output vector \mathbf{o} is denoted as P , with $P(\mathbf{o})$ the probability for the computational outcome \mathbf{o} .

In this paper, we consider two notions of classically simulating MBQCs, namely

1. Computing the elements $P(\mathbf{o})$ of P exactly, for arbitrary output values \mathbf{o} .
2. Sampling from the probability distribution P .

Consider the scenario where either a measurement-based quantum computer or a classical device simulating it is hidden behind a wall, and one is supposed to figure out the identity of the device merely by looking at its output.

It is possible to distinguish the real quantum computer from a classical device efficiently simulating MBQC according to the first notion, e.g. by setting up a problem where $P(\mathbf{o}) = \delta(\mathbf{o}, \mathbf{m})$, for some \mathbf{m} ; i.e., a needle in a haystack. If the classical device could only compute $P(\mathbf{o})$ efficiently for each \mathbf{o} , it would still generally require exponential time in the length of \mathbf{o} to find the correct output \mathbf{m} .

However, it is not possible to distinguish a quantum computer from a device efficiently simulating MBQC according to the second criterion, since the probability distribution P fully characterizes the output of the computation. Indeed, the quantum computer itself samples from P [24].

The probability of obtaining a particular sequence of measurement outcomes on all of the $|E|$ qubits is $|\langle \mathcal{R} | \phi \rangle|^2$, where $|\phi\rangle$ is a tensor product of single qubit outcome states. In general, the ability to compute $\langle \mathcal{R} | \phi \rangle$ is sufficient for classical simulation of the first type, since the $P(\mathbf{o})$ are all expressible in the form $|\langle \mathcal{R} | \phi \rangle|^2$. Yet, the ability to compute a single such inner product efficiently is not sufficient for efficient classical simulation via sampling from P , as the above example illustrates. It

is possible however to efficiently sample from P if partial measurement probabilities

$$p(|\phi_{\tilde{E}}\rangle) = \text{tr}_{\tilde{E}}(\langle \phi_{\tilde{E}} | \mathcal{R} \rangle \langle \mathcal{R} | \phi_{\tilde{E}} \rangle)$$

can be computed efficiently. Therein, \tilde{E}, \hat{E} is a bipartition of the qubits E into a set of measured qubits \tilde{E} and unmeasured qubits \hat{E} , and $|\phi_{\tilde{E}}\rangle := \otimes_{e \in \tilde{E}} |\phi_e\rangle$ is a post-measurement state on the measured qubits, representing the outcomes obtained. Consider a step of MBQC where the next qubit to be measured is some $e \in \hat{E}$. If one now computes $p(|\phi_{\tilde{E}}\rangle \otimes |\phi_e\rangle)$, then Bayes' formula yields the probability of obtaining $|\phi_e\rangle$ for qubit e , conditioned on the past measurement results:

$$p(|\phi_e\rangle \mid |\phi_{\tilde{E}}\rangle) = \frac{p(|\phi_{\tilde{E}}\rangle \otimes |\phi_e\rangle)}{p(|\phi_{\tilde{E}}\rangle)}.$$

In this way, one can simulate MBQC by only sampling from distributions over two outcomes, one time for each qubit $e \in E$. If $p(|\phi_{\tilde{E}}\rangle)$ can be computed in a number of steps that scales polynomially in $|E|$, at each step \tilde{E} of the computation, then the whole simulation can be performed in $\text{poly}(\tilde{E})$ time.

In our context, we will focus initially on the computation of complete local state inner products $\langle \bar{\psi} | \phi \rangle$, where $|\bar{\psi}\rangle$ is a surface-code state, and $|\phi\rangle$ is a product state. We will then find in Section V that for a certain family of arbitrary genus graphs and a natural ordering of measurements, the task of computing partial measurement probabilities $p(|\phi_{\tilde{E}}\rangle)$ reduces to a special case of evaluating $\langle \bar{\psi} | \phi \rangle$.

IV. PRODUCT STATE OVERLAPS AND ENTANGLEMENT

A. Product state overlaps and the Ising model

We will begin by showing that the inner product between any surface-code state and an arbitrary product state can be written as a sum of classical Ising model partition functions. Consider any product state in the physical Hilbert space of the $|E|$ qubits:

$$|\phi\rangle = \bigotimes_{e \in E} (a_e |0\rangle_e + b_e |1\rangle_e).$$

The inner product between $|\phi\rangle$ and the encoded X eigenstate $|\bar{\psi}\rangle$ of Equation 1 can be written as a summation over the set $E_0(G)$:

$$\begin{aligned} \langle \bar{\psi} | \phi \rangle &= \frac{1}{\sqrt{|E_0(G)|}} \sum_{x \in E_0(G)} \langle x | \left(\bigotimes_{e \in E} a_e |0\rangle_e + b_e |1\rangle_e \right) \\ &= \frac{1}{\sqrt{|E_0(G)|}} \left(\prod_{e \in E} a_e \right) \sum_{x \in E_0(G)} \prod_{e \in E} \left(\frac{b_e}{a_e} \right)^{x_e}, \quad (3) \end{aligned}$$

where if $a_e = 0$ for any edge e we take a limit as $a_e \rightarrow 0$ and use the continuity of $\langle \bar{\psi} | \phi \rangle$ as function of the a_e and b_e .

The state overlap in Equation 3 is proportional to the partition function of a classical Ising model with classical spins $\sigma_v \in \{0, 1\}$ on the vertices of G , and possibly complex couplings $J_e = \tanh^{-1}(\frac{b_e}{a_e})$ associated with each edge. It is well known (see [25] and [26]) that the partition function of an Ising model defined on a graph G with couplings J_e can be written as a generating function of cycles on G :

$$Z(G, J) = 2^{|V|} \left(\prod_{e \in E} \cosh(J_e) \right) \text{Cy}(G, \tanh(J)), \quad (4)$$

where

$$\text{Cy}(G, w) := \sum_{x \in E_0(G)} \prod_{e \in E} (w_e)^{x_e}$$

is the generating function of cycles on G , where a weight w_e is associated with each edge e . Comparing Equations 3 and 4, we see that if we define the Ising couplings as $J_e := \tanh^{-1}(\frac{b_e}{a_e})$, then

$$\langle \bar{\psi} | \phi \rangle = \frac{\prod_{e \in E} \sqrt{a_e^2 - b_e^2}}{2^{|V|} \sqrt{|E_0(G)|}} Z(G, J). \quad (5)$$

Now consider any state $|\bar{\psi}\rangle$ in the surface-code space, with expansion coefficients c_γ in the encoded X eigenbasis: $|\bar{\psi}\rangle = \sum_{\gamma \in \{0,1\}^{\otimes 2g}} c_\gamma |\bar{X}_\gamma\rangle$. Expanding the inner product in this basis

$$\langle \bar{\psi} | \phi \rangle = \sum_{\gamma \in \{0,1\}^{\otimes 2g}} c_\gamma^* \langle \bar{\psi} | \left(\prod_{j=1}^{2g} \bar{Z}_j^{\gamma_j} \right) | \phi \rangle. \quad (6)$$

Recall that the encoded Pauli Z operators are tensor products of Pauli Z operators acting on the physical qubits. If we take them as operating to the right rather than the left in Equation 6, then we see that each term is proportional to an inner product between $|\bar{\psi}\rangle$ and a modified product state $|\phi^\gamma\rangle := \left(\prod_{j=1}^{2g} \bar{Z}_j^{\gamma_j} \right) |\phi\rangle$. So we could write Equation 6 as a summation over 2^{2g} Ising partition functions, each with different Ising couplings defined from the coefficients of $|\phi^\gamma\rangle$. However, we will find it useful to keep each term in the form of Equation 3:

$$\begin{aligned} \langle \bar{\psi} | \phi \rangle &= \mathcal{N} \sum_{\gamma \in \{0,1\}^{\otimes 2g}} c_\gamma^* \sum_{x \in E_0(G)} \prod_{e \in E} \left(\frac{b_e^\gamma}{a_e} \right)^{x_e} \\ &= \mathcal{N} \sum_{\gamma \in \{0,1\}^{\otimes 2g}} c_\gamma^* \text{Cy}(G, w^\gamma), \end{aligned} \quad (7)$$

where $\mathcal{N} := \frac{\prod_{e \in E} a_e}{\sqrt{|E_0(G)|}}$ and b_e^γ is obtained from b_e by letting $b_e \rightarrow -b_e$ each time the edge e belongs to a cocycle C'_j such that $\gamma_j = 1$. The weights w^γ are defined as $w_e^\gamma := b_e^\gamma / a_e$.

B. Evaluation of product state overlaps

From Equation 7, we see that in order to compute an inner product of the form $\langle \bar{\psi} | \phi \rangle$, it is sufficient to be able to evaluate a generating function of cycles on G . Note that the generating function of cycles of a graph G depends only on its vertex and edge sets V and E , and makes no reference to an embedding of G on any surface. However, it turns out that embedding G on an orientable surface of genus g allows one to compute $\text{Cy}(G, w)$ in a number of steps that grows exponentially in g , while only polynomially in the size of the graph.

In Appendix A, we show that for a graph G embedded on an orientable surface of genus g , the generating function of cycles on G can be written as

$$\text{Cy}(G, w) = \frac{1}{2^g} \sum_{\alpha, \beta \in \{0,1\}^{\otimes g}} (-1)^{\alpha \cdot \beta} \text{Pf}(\mathcal{A}'(w^{\alpha, \beta})), \quad (8)$$

where $\alpha \cdot \beta$ is the bitwise inner product of the g component bitstrings α and β , and $\text{Pf}(\mathcal{A}'(w))$ is the Pfaffian of the weighted adjacency matrix of a modified graph G' , which is obtained from the graph G with edge weights w . Here, $w^{\alpha, \beta}$ indicates the set of edge weights of G adjusted in a certain way that depends on the bitstrings α and β . The Pfaffian of a matrix is related to the determinant and is computable in a number of steps that grows polynomially in the size of the matrix. The number of edges of G' is a polynomial in the number of edges of G , so $\text{Pf}(\mathcal{A}'(w^{\alpha, \beta}))$ can be computed efficiently in both the number of edges and the genus g . Equation 8 allows for an evaluation of $\text{Cy}(G, w)$ in $\text{poly}(|E|, g) 2^{2g}$ steps.

The construction of the adjusted edge weights $w^{\alpha, \beta}$ will be crucial in the following considerations. In Appendix A, we define a *canonical encoding scheme*, which is a possible choice of encoding cocycles C'_k defined by cutting and then unfolding the surface S into a topological disk. In a canonical encoding scheme, the numbering of cocycles $C'_1 \dots C'_{2g}$ is important; in particular, each odd numbered cocycle C'_{2j-1} is paired with an even numbered cocycle C'_{2j} . Given a canonical encoding scheme $C'_1 \dots C'_{2g}$, $w_e^{\alpha, \beta}$ is defined from w_e by multiplying w_e by -1 each time e belongs to an odd numbered cocycle C'_{2j-1} such that $\alpha_j = 1$, and each time e belongs to an even numbered cocycle C'_{2j} such that $\beta_j = 1$.

Consider now the coefficients $c_{\gamma, \rho}$ of an encoded state with respect to a canonical encoding scheme C'_k , where $\gamma, \rho \in \{0,1\}^{\otimes g}$, γ_j corresponds to the odd numbered cocycle C'_{2j-1} , and ρ_j to the even numbered cocycle C'_{2j} . Then we may re-write Equation 7 as

$$\langle \bar{\psi} | \phi \rangle = \mathcal{N} \sum_{\gamma, \rho \in \{0,1\}^{\otimes g}} c_{\gamma, \rho}^* \text{Cy}(G', w^{\gamma, \rho}).$$

The bitstrings γ, ρ modify the edge weights w_e here in exactly the same way as the bitstrings α, β do in Equation 8. So substituting in Equation 8:

$$\langle \bar{\psi} | \phi \rangle = \frac{\mathcal{N}}{2^g} \sum_{\substack{\alpha, \beta, \gamma, \rho \\ \in \{0,1\}^{\otimes g}}} c_{\gamma, \rho}^* (-1)^{\alpha \cdot \beta} \text{Pf}(\mathcal{A}'(w^{\alpha \oplus \gamma, \beta \oplus \rho})),$$

where \oplus indicates here the binary sum of two bitstrings. By re-labelling the summation over the dummy indices α, β , we can rewrite

$$\langle \bar{\psi} | \phi \rangle = \frac{\mathcal{N}}{2^g} \sum_{\substack{\alpha, \beta, \gamma, \rho \\ \in \{0,1\}^{\otimes g}}} c_{\gamma, \rho}^* (-1)^{(\alpha \oplus \gamma) \cdot (\beta \oplus \rho)} \text{Pf}(\mathcal{A}'(w^{\alpha, \beta})), \quad (9)$$

where \mathcal{N} is as defined in Section III. Equation 9 provides a means of computing $\langle \bar{\psi} | \phi \rangle$ in a number of steps that scales as $\text{poly}(|E|, g)2^{4g}$.

There exists a family of states in the code space of a surface-code for which the two summations in Equation 9 cancel each other out, and the complexity of evaluating product state overlaps loses its exponential dependence on g . Consider a state $|\bar{C}^{\delta, \epsilon}\rangle$ parameterized by two g -component bitstrings δ, ϵ :

$$|\bar{C}^{\delta, \epsilon}\rangle := \frac{1}{2^g} \sum_{\gamma, \rho \in \{0,1\}^{\otimes g}} (-1)^{\delta \cdot \rho + \epsilon \cdot \gamma + \gamma \cdot \rho} |\bar{X}_{\gamma, \rho}\rangle, \quad (10)$$

where $|\bar{X}_{\gamma, \rho}\rangle$ is the encoded X basis defined by some fixed canonical encoding scheme. It can be verified directly that

$$\begin{aligned} & \frac{1}{2^g} \sum_{\gamma, \rho \in \{0,1\}^{\otimes g}} (-1)^{\delta \cdot \rho + \epsilon \cdot \gamma + \gamma \cdot \rho} (-1)^{(\alpha \oplus \gamma) \cdot (\beta \oplus \rho)} \\ &= \frac{1}{2^g} (-1)^{\alpha \cdot \beta} \sum_{\gamma, \rho \in \{0,1\}^{\otimes g}} (-1)^{\gamma \cdot (\epsilon \oplus \beta) + \rho \cdot (\delta \oplus \alpha)} \end{aligned}$$

equals zero unless $\alpha = \delta$ and $\beta = \epsilon$ component by component, in which case it equals $(-1)^{\delta \cdot \epsilon} 2^g$. So, using Equation 9:

$$\langle \bar{C}^{\delta, \epsilon} | \phi \rangle = \mathcal{N} (-1)^{\delta \cdot \epsilon} \text{Pf}(\mathcal{A}'(w^{\delta, \epsilon})), \quad (11)$$

which can be computed in $\text{poly}(|E|, g)$ time. The states $|\bar{C}^{\delta, \epsilon}\rangle$ are the encodings of a state that is locally equivalent to a graph state of tensor product form, with one factor per handle. Each handle of the surface S encodes two qubits, and the corresponding graph state is local equivalent to a Bell state; see Figure 3. The state $|\bar{C}^{\delta, \epsilon}\rangle$ has stabilizers $(-1)^{\delta_j} \bar{X}_{2j-1} \bar{Z}_{2j}$ and $(-1)^{\epsilon_j} \bar{Z}_{2j-1} \bar{X}_{2j}$, for each $j = 1 \dots g$.

The 2^{2g} states $|\bar{C}^{\delta, \epsilon}\rangle$ form an orthonormal basis for the code space of the surface code, which can be proven using the orthonormality of the encoded X eigenstates. If the coefficients $\psi_{\delta, \epsilon}$ expanding an arbitrary surface-code state $|\bar{\psi}\rangle$ in the $|\bar{C}^{\delta, \epsilon}\rangle$ basis are known:

$$|\bar{\psi}\rangle = \sum_{\delta, \epsilon \in \{0,1\}^{\otimes g}} \psi_{\delta, \epsilon} |\bar{C}^{\delta, \epsilon}\rangle,$$

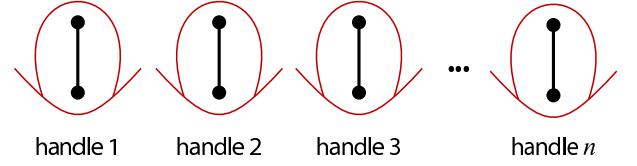


FIG. 3: (Color online) The states in the code space for which MBQC remains efficiently simulatable are encodings of graph states. The graph has multiple components, one per handle. Each handle gives rise to two encoded qubits, and the graph state on each handle is locally equivalent to a Bell state among these two qubits.

then we can improve upon Equation 9 to compute $\langle \bar{\psi} | \phi \rangle$ in a number of steps that scales as $\text{poly}(|E|, g)2^{2g}$:

$$\langle \bar{\psi} | \phi \rangle = \mathcal{N} \sum_{\alpha, \beta \in \{0,1\}^{\otimes g}} (-1)^{\alpha \cdot \beta} \psi_{\alpha, \beta}^* \text{Pf}(\mathcal{A}'(w^{\alpha, \beta})). \quad (12)$$

This observation leads us to the following

Theorem IV.1 *Consider an MBQC with generalized flow on a resource surface-code state $|\bar{\psi}\rangle = \sum_{\alpha, \beta \in \mathbb{Z}_2^g} \psi_{\alpha, \beta} |\bar{C}^{\alpha, \beta}\rangle$ of $|E|$ qubits, where g is the genus, and the coefficients $\psi_{\alpha, \beta}$ are known. Then, each element $P(\mathbf{o})$ of the output probability distribution can be computed exactly in $2^{2g} \text{Poly}(|E|, g)$ steps.*

Remark: A generalized flow consists of a partial ordering among the individual measurement events and a rule for working out which measurement basis depends on which measurement outcome obtained earlier. For a precise definition, see [27]. The extra condition of the MBQC possessing a generalized flow does not seem very constraining, since it is the only known condition that guarantees deterministically runnable MBQC.

Proof By Theorem 2 of [27], the property of a generalized flow implies strong determinism of the MBQC in question, meaning that each branch of the MBQC is equally likely. We may now split the set Ω of qubits into two disjoint subsets O and $O^c := \Omega \setminus O$, where O^c is the set of qubits which condition a correction operation and O the set of qubits which do not. The latter are the output qubits, and can be measured last.

The standard procedure of MBQC with all qubits being measured and the output bits obtained as parities of measurement outcomes is equivalent to the following procedure [28]: (1) Putting in place the resource state. (2) Performing the local measurements on all qubits $a \in O^c$. (3) Applying Pauli operators on the remaining qubits $b \in O$, conditioned upon the measurement outcomes obtained on the qubits $a \in O^c$. The resulting state of the unmeasured qubits is $|\text{out}\rangle_O$. (4) Measuring all qubits $b \in O$. Each measurement outcome yields one bit o_b of output, for all $b \in O$.

By Theorem 2 of [27], the state $|\text{out}\rangle_O$, outputted in step 3 of the above procedure, is independent of the measurement outcomes $\mathbf{s}|_{O^c}$ of qubits in O^c , and all combinations $\mathbf{s}|_{O^c}$ of local measurement outcomes are equally likely. Therefore, it is not necessary to compute each of these probabilities separately. Instead, one may set $\mathbf{s}|_{O^c} = \mathbf{0}|_{O^c}$. In this case, there are no Pauli corrections on the qubits in O . Furthermore,

$$P(\mathbf{o}) = 2^{|O^c|} |\langle \bar{\psi} | \mathbf{0} \rangle_{O^c} | \mathbf{o} \rangle_O|^2. \quad (13)$$

Therein, $|\mathbf{0}\rangle_{O^c}$ is the post-measurement state on the qubits in O^c , with every measurement outcome being $s_a = 0$ (eigenvalue +1), for all $a \in O^c$. $|\mathbf{o}\rangle_O$ is the post-measurement state of the qubits in O , with $s_b = o_b$, for all $b \in O$. (In both cases, the basis of the measurement is specified through the algorithm. It is in general not the computational basis.)

Now, by Eq. (12), the probability $P(\mathbf{o})$ can be computed as a sum over 2^{2g} terms. In each term, $\text{Pf}(\mathcal{A}'(w^{\alpha,\beta}))$ can be computed in $\text{Poly}(|E|, g)$ steps. \square

C. Quantum circuit interpretation

Another perspective on the perhaps surprising efficiency of the states $|\bar{C}^{\delta,\epsilon}\rangle$ comes from thinking of the evaluation of $\langle \bar{\psi} | \phi \rangle$ as equivalent to computing a matrix element of a quantum circuit that entangles a set of N non-interacting fermions to $2g$ qubits (see Figure 4). This interpretation is possible in certain situations where the graph G corresponds to a higher genus analog of a rectangular lattice with N rows, such as the punctured cylinder graphs to be introduced in Section V B. In this case, the Ising model partition function can be evaluated by a simple generalization of the transfer matrix method.

For an $N \times M$ rectangular lattice, the transfer matrix method [29] allows the Ising model partition function to be written as the vacuum expectation value of a non-interacting fermion operator on N fermion modes:

$$Z = 2^N \langle \text{vac} | V^1 H^1 \dots V^{M-1} H^{M-1} V^M | \text{vac} \rangle$$

where $V^1 \dots V^M$ are known as vertical transfer matrices, expressed as non-interacting fermion operators with parameters that depend on the vertical Ising couplings along a given column of the lattice, while the H_j are non-interacting fermion operators that depend on the horizontal couplings down a given column. This leads to an interpretation of the partition function in terms of a 1D quantum system, where the horizontal dimension acts as time. For certain suitably “rectangular” non-planar graphs [30], this formula can be generalized as

$$Z = \frac{1}{2^g} \sum_{\alpha, \beta \in \{0,1\}^{\otimes g}} (-1)^{\alpha \cdot \beta} \langle \text{vac} | \Gamma_{\alpha, \beta} | \text{vac} \rangle \quad (14)$$

where $\Gamma_{\alpha, \beta}$ is again a product of non-interacting fermion operators, which depend on the bitstrings α and

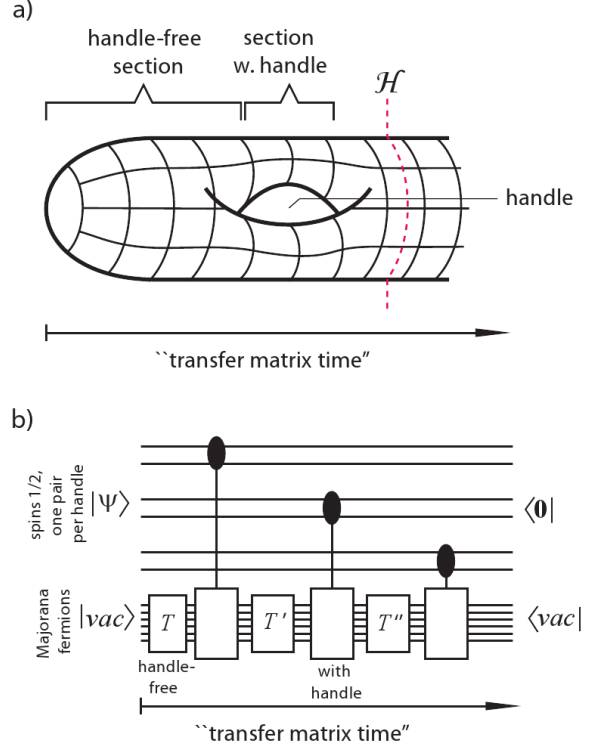


FIG. 4: (Color online) Quantum circuit representation of the computation of a surface-code inner-product $\langle \bar{\psi} | \phi \rangle$ for appropriate graphs. In figure b), the encoded state $|\psi\rangle$ is loaded into a register of $2g$ qubits, where it is subsequently entangled with a set of N non-interacting fermions that evolve conditional on the state of the qubits. The interaction is diagonal in the $|\bar{C}^{\delta,\epsilon}\rangle$ basis of the qubits.

β as the virtual time evolution crosses handles in the surface from left to right (see Figure 4).

The $2g$ bits α, β arise because non-planar vertical boundary conditions (such as those depicted in Figure 4) alter the normal mapping from transfer matrices to non-interacting fermion operators via the Jordan-Wigner transformation. To express the product of transfer matrices in terms of non-interacting fermion operators, it is necessary to sum over various parity subspaces of the fermion Fock space, which leads to the summation in Equation 14. The vertical transfer matrices corresponding to edge qubits directly above a handle take a form $e^{-iJ(-1)^{\hat{n}_k} c_{2k} c_1} = P_k^- e^{iJ c_{2k} c_1} + P_k^+ e^{-iJ c_{2k} c_1}$ where \hat{n}_k counts the occupation of the subset of fermion modes $1-k$, and P_k^\pm is the projector into the positive(negative) parity eigenspace of \hat{n}_k . The $c_1 \dots c_{2N}$ are Majorana fermion operators and J is a scalar Ising coupling. The parity projectors themselves can each be expanded as $P_k^\pm = \frac{1}{2} (I \pm (-1)^{\hat{n}_k})$, where the action of the operator $(-1)^{\hat{n}_k}$ in the second term turns out to be equivalent to multiplying by -1 the horizontal Ising couplings for edges immediately to the left of the handle. Thus in term $\Gamma_{\alpha, \beta}$

of Equation 14, both α_j and β_j are associated with the signs of certain Ising couplings around the j^{th} handle.

When this method for computing the Ising partition function is used for the computation of a surface-code inner-product, we get that

$$\langle \phi | \bar{\psi} \rangle \propto \langle vac \otimes \mathbf{0} | CT | vac \otimes \psi \rangle. \quad (15)$$

where CT is a “controlled” fermion operator:

$$CT := \sum_{\alpha, \beta \in \{0,1\}^{\otimes g}} |C^{\alpha, \beta}\rangle \langle C^{\alpha, \beta}| \otimes \Gamma_{\alpha, \beta}.$$

Therein, $|\psi\rangle$ is the $2g$ -qubit state being encoded into the surface code, and $|\mathbf{0}\rangle$ is the computational basis state on the qubits. Non-interacting fermion operators can be efficiently classically simulated (even when they are non-unitary), so Equation 15 can be evaluated in a number of steps that depends on the number of terms in an expansion of the state $|\psi\rangle$ in the $|C^{\alpha, \beta}\rangle$ basis. In particular, if $|\bar{\psi}\rangle = |\bar{C}^{\delta, \rho}\rangle$ for some δ, ρ , then only one term must be computed and the evaluation of Equation 15 is efficient in all parameters. For more details on this approach, see [30].

D. Entanglement in the effective output state

In the following we will prove tighter bounds on the classical simulation cost on MBQC with surface-code states, in which the exponential factor 2^{2g} in Theorem IV.1 is replaced by smaller exponentials. Specifically, we have

$$2^{E_{Sch}(|\Phi\rangle)} \leq 2^{n(|\Phi\rangle)} \leq 2^{2g},$$

where $|\Phi\rangle$ is an effective state containing all relevant information about the encoded state $|\psi\rangle$, the encoding and the local bases in which $|\bar{\psi}\rangle$ is measured. Furthermore, E_{Sch} is the Schmidt measure of entanglement and n is the log of the number of terms in a special fixed basis expansion. We have already seen that n can be much smaller than $2g$, namely $n = 0$ for the graph states in Fig. 3. Our tightest bound involves the Schmidt entanglement measure, and is stated in Theorem IV.2. A complication arises due to the fact that computing the optimal basis for the Schmidt decomposition in general is a hard problem in itself. In this regard, we show that $E_{Sch}(|\Phi\rangle) = n(|\Phi\rangle)$ under mild assumptions; See Theorem IV.3.

Recall that the states $|\bar{C}^{\alpha, \beta}\rangle$ can be written in terms of the encoded X-eigenstates of a canonical encoding scheme:

$$|\bar{C}^{\alpha, \beta}\rangle := \frac{1}{2^g} \sum_{\gamma, \rho \in \{0,1\}^{\otimes g}} (-1)^{\alpha \cdot \rho + \beta \cdot \gamma + \gamma \cdot \rho} |\bar{X}_{\gamma, \rho}\rangle.$$

It is straightforward to prove that these states are all related to one another by encoded Pauli Z operators for

a canonical encoding scheme. In particular

$$|\bar{C}^{\alpha, \beta}\rangle = (-1)^{\alpha \cdot \beta} \left(\prod_{j=1}^g (\bar{Z}_{2j-1})^{\alpha_j} (\bar{Z}_{2j})^{\beta_j} \right) |\bar{C}^{0,0}\rangle,$$

where $|\bar{C}^{0,0}\rangle$ indicates the state labeled by the g -component zero bitstring for both α and β , and $\bar{Z}_k = \prod_{e \in C'_k} Z_e$. To simplify notation, define

$$\Psi_{\alpha, \beta} := (-1)^{\alpha \cdot \beta} \psi_{\alpha, \beta}^*.$$

Then we can write any state in the surface-code space as

$$|\bar{\psi}\rangle = \sum_{\alpha, \beta} \Psi_{\alpha, \beta}^* \left(\prod_{k=1}^g \bar{Z}_{2k-1}^{\alpha_k} \bar{Z}_{2k}^{\beta_k} \right) |\bar{C}^{00}\rangle.$$

(Note that we have suppressed the $\in \{0,1\}^{\otimes g}$ under the summation sign to clean up the expression.)

Now consider the quantity $\langle \bar{\psi} | \phi \rangle$. If we let the Pauli Z operators operate to the right rather than the left we see that

$$\langle \bar{\psi} | \phi \rangle = \langle \bar{C}^{00} | \Phi \rangle,$$

where

$$\begin{aligned} |\Phi\rangle &:= \sum_{\alpha, \beta} \Psi_{\alpha, \beta} \left(\prod_{k=1}^g \bar{Z}_{2k-1}^{\alpha_k} \bar{Z}_{2k}^{\beta_k} \right) |\phi\rangle \\ &= \sum_{\alpha, \beta} \Psi_{\alpha, \beta} \left(\prod_{k=1}^g \prod_{e \in C'_{2k-1}} Z_e^{\alpha_k} \prod_{e \in C'_{2k}} Z_e^{\beta_k} \right) \bigotimes_{e \in E} |\phi_e\rangle. \end{aligned} \quad (16)$$

Thus, evaluating the overlap between an arbitrary surface-code state and a product state is equivalent to evaluating the overlap of one of the “easy” states $|\bar{C}^{00}\rangle$ with an effective state $|\Phi\rangle$ which is generally *not* a product state of the physical qubits. In a sense, the state $|\Phi\rangle$ reflects an encoding of the $2g$ qubit state $|\psi\rangle$ into the $|E|$ physical qubits of the state $|\phi\rangle$. From Equation 16, it is clear that $|\Phi\rangle$ is a function of: i) the state $|\psi\rangle$ being encoded into the surface code; ii) the chosen encoding scheme $C'_1 \dots C'_{2g}$; and iii) the product state $|\phi\rangle$. In terms of simulating MBQC, the state $|\Phi\rangle$ combines both the specification of the resource state and the particular sequence of measurement outcomes one is computing the probability of (see Section III).

If $|\Phi\rangle$ were to be expanded as a sum over product states, we could evaluate $\langle \bar{C}^{00} | \Phi \rangle$ in a number of steps that grows linearly with the number of terms in the expansion. The base-2 logarithm of the minimal number of product states that are required to expand a multipartite quantum state is an entanglement monotone known as the *Schmidt measure* [31]. That is, for an N qubit pure

state $|\psi\rangle$, the Schmidt measure $E_{Sch}(|\psi\rangle)$ is the minimum number such that

$$|\psi\rangle = \sum_{j=1}^{2^{E_{Sch}(|\psi\rangle)}} |\chi_1^j\rangle |\chi_2^j\rangle \dots |\chi_N^j\rangle$$

for some set of local states $|\chi_k^j\rangle$ for all $j = 1 \dots 2^{E_{Sch}(|\psi\rangle)}$, $k = 1 \dots N$. We will call the $|\chi_k^j\rangle$ in such an expansion (with $2^{E_{Sch}(|\psi\rangle)}$ terms) an *optimal local basis* for $|\psi\rangle$. Applying the Schmidt measure to our situation, we immediately have the following result.

Theorem IV.2 *If an optimal local basis for the effective state $|\Phi\rangle$ is known, then $\langle\bar{\psi}|\phi\rangle$ can be computed in a number of steps that scales as $\text{poly}(|E|, g)2^{E_{Sch}(|\Phi\rangle)}$.*

Computation of $E_{Sch}(|\psi\rangle)$ for a generic multipartite state - no less finding an optimal local basis for it - is generally a very hard problem. Yet an efficient means of computing an optimal local basis is necessary to give Theorem IV.2 much practical significance. In our case, the task of evaluating the Schmidt measure is simplified considerably by the definition of $|\Phi\rangle$. Since each term Equation 16 is a product state, we know that $E_{Sch}(|\Phi\rangle)$ must be less than or equal to $2g$, even though $|\Phi\rangle$ is a state on generally many more than $2g$ qubits. Furthermore, we can show that under fairly general conditions, Equation in fact 16 already provides an optimal local basis for $|\Phi\rangle$.

To state these conditions, we briefly introduce some notation. Let $G - Z$ denote the subgraph of G composed of all edges e such that $|\phi_e\rangle$ is not a Pauli Z eigenstate. For any set of edges \mathbf{A} , let $M_{\mathbf{A}}$ be an $|\mathbf{A}| \times 2g$ matrix such that $M_{e,k} = 1$ if $e \in C'_k$ and $M_{e,k} = 0$ if $e \notin C'_k$, for all $e \in \mathbf{A}$. Note that there must exist some edge set $\mathbf{A} = \{e_k\}_{k=1 \dots 2g}$ such that $\text{rank}(M_{\mathbf{A}}) = 2g$ over the binary field, since the cocycles C'_k are mutually independent as edge sets. For the theorem, we will need to assume a slightly stronger condition:

Theorem IV.3 *Consider the case where $G - Z$ contains two disjoint sets of $2g$ edges $\mathbf{A} = \{e_k\}_{k=1 \dots 2g}$ and $\mathbf{B} = \{e'_k\}_{k=1 \dots 2g}$ such that $\text{rank}(M_{\mathbf{A}}) = \text{rank}(M_{\mathbf{B}}) = 2g$. Then the expansion in Equation 16 yields an optimal local basis for $|\Phi\rangle$ and $E_{Sch}(|\Phi\rangle) = \log_2(D)$, where D is the number of nonzero coefficients Ψ_{α} .*

Proof See Appendix B.

The condition assumed for Theorem IV.3 seems very weak in practice, but in principle may not hold. Figure 5 shows a simple embedded graph with cocycles C'_k that would violate the condition if any of the cocycle edges were measured in the Z-eigenbasis.

The state $|\Phi\rangle$ and the coefficients $\Psi_{\alpha,\beta}$ can be efficiently computed from the coefficients $\psi_{\alpha,\beta}$ and the definition of the surface-code cocycles C'_k . The number of nonzero $\Psi_{\alpha,\beta}$ is exactly equal to the number of nonzero

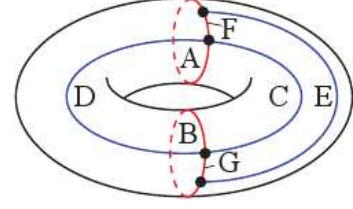


FIG. 5: An embedded graph for which the condition of Theorem IV.3 does not hold, if one uses cocycles $C'_1 = \{C, E\}$, $C'_2 = \{A, B\}$, and for at least one edge $e \in \{A, B, C, E\}$ the state $|\phi_e\rangle$ is a Z-eigenstate.

$\psi_{\alpha,\beta}$. It follows from Theorem IV.3 then that if the D nonzero coefficients $\psi_{\alpha,\beta}$ are known, and the assumption of the theorem is satisfied, then the quantity $\langle\bar{\psi}|\phi\rangle$ can be evaluated in a number of steps that is polynomial in the size and genus of the embedded graph but increases exponentially with the entanglement in $|\Phi\rangle$, as measured by the Schmidt number. We remark that the assumption of Theorem IV.3 is satisfied whenever the restriction of each C'_k to $G - Z$ contains two edges that are not shared with any of the other C'_l for $l \neq k$, which would be expected of cocycles on any but the smallest graphs.

V. PARTIAL MEASUREMENT PROBABILITIES

In this section we turn to classical simulation in the strong sense of notion 2 in Section III. As a starting point, we recall the result from [15], in which it was shown that MBQC on surface-code states can be efficiently simulated when the underlying graph is planar, and the set of measured qubits \tilde{E} and its complement \hat{E} are connected at all stages of computation. This result is demonstrated by showing that the probability of obtaining a particular sequence of measurement outcomes on \tilde{E} is proportional to the inner product between a planar code state on a modified graph $G_{\tilde{E}} \cup G_{\tilde{E}}^*$ and a product state. The graph $G_{\tilde{E}} \cup G_{\tilde{E}}^*$ is obtained by taking two copies of the subgraph $G_{\tilde{E}}$ and gluing them together at the boundary of \tilde{E} and \hat{E} .

We will obtain a similar result for general surface-code states, but in the present context the relation is considerably complicated due to the nontrivial topology of $G_{\tilde{E}} \cup G_{\tilde{E}}^*$. To handle this new setting, we find it necessary to specialize to cases where underlying graph is what we will call a *punctured cylinder graph* of genus g . In doing so, we find that MBQC on a punctured cylinder graph surface code with a natural ordering of single qubit measurements can be simulated (in the strong sense) efficiently in the size of the graph, but inefficiently in g . For the states $|\tilde{C}^{\alpha,\beta}\rangle$ in this code space, the simulation is completely efficient.

While we expect the result to extend to more general

surface-code states and measurement orders, we were unable to prove such as result, and leave it as an open question. Punctured cylinder graphs represent a very simple generalization of the square lattice to higher genus. Furthermore, as a family they contain all higher genus graphs as a graph minor. In principle this makes most of our analysis applicable to arbitrary graphs (see the footnote and discussion of graph minor operations in Section C 2), but it is unclear what efficiencies hold in general.

A. General considerations

We consider simulating MBQC by computation of the partial measurement probabilities introduced in Section III:

$$p(|\phi_{\tilde{E}}\rangle) = \text{tr}_{\tilde{E}}(|\phi_{\tilde{E}}\rangle\langle\psi|\langle\psi|\phi_{\tilde{E}}\rangle).$$

We will begin by proving some results regarding $p(|\phi_{\tilde{E}}\rangle)$ that hold for all connected graphs G with no self loops. In what follows, we will assume as in [15] that at each stage of the computation, the set of measured edges \tilde{E} is connected, as is the set of unmeasured edges \hat{E} . Our first step will be to construct a Schmidt decomposition for the state $|\bar{\tau}\rangle$. This will follow from a few definitions and lemmata.

Let $G(\tilde{E})$ denote the subgraph of G that contains only the edges \tilde{E} , as well as all vertices \tilde{V} which have at least one edge incident on them from the set \tilde{E} . Define \hat{V} and $G(\hat{E})$ similarly, and let $\partial\tilde{E} \subseteq V := \tilde{V} \cap \hat{V}$ be the set of vertices containing at least one edge incident upon it from both of the sets \tilde{E} and \hat{E} . We can think of $\partial\tilde{E}$ as the boundary between the sets \tilde{E} and \hat{E} .

Let $E_0(\tilde{E})$ denote the set of cycles on the graph $G(\tilde{E})$, and define $E_0(\hat{E})$ analogously. Under the assumption that \tilde{E} is connected, we have:

Lemma V.1 $|E_0(\tilde{E})| = 2^{|\tilde{E}| - |\tilde{V}| + 1}$.

Proof $E_0(\tilde{E})$ is a set of $|\tilde{E}|$ binary variables $\{x_e\}$ satisfying the $|\tilde{V}|$ binary equations: $\sum_{e \in \delta_s} x_e = 0$ for all $s \in \tilde{V}$. If we add together the equation $\sum_{e \in \delta_s} x_e = 0$ over all $s \in \tilde{V}$, then each binary variable x_e appears either twice or not at all, and we obtain $0 = 0$. The equations are otherwise bitwise linearly independent so the total number of independent binary equations is $|\tilde{V}| - 1$. \square

Now let $E_0(\tilde{E}, \partial\tilde{E})$ denote the set of binary strings over the edges such that the cycle condition holds everywhere except possibly on the vertices on the boundary $\partial\tilde{E}$.

Lemma V.2 $|E_0(\tilde{E}, \partial\tilde{E})| = 2^{|\tilde{E}| - |\tilde{V}| + |\partial\tilde{E}|}$.

Proof $E_0(\tilde{E})$ is a set of $|\tilde{E}|$ binary variables $\{x_e\}$ satisfying the $|\tilde{V}| - |\partial\tilde{E}|$ binary equations: $\sum_{e \in \delta_s} x_e = 0$ for all $s \in \tilde{V} \setminus \partial\tilde{E}$. The exclusion of the vertices in $\partial\tilde{E}$ removes any linearly dependence among these equations. \square

We now turn to the structure of the set $E_0(\tilde{E}, \partial\tilde{E})$. For any $\tilde{x} \in E_0(\tilde{E}, \partial\tilde{E})$, let $\Delta\tilde{x}$ be a bitstring encoding the parity of edges from \tilde{x} incident on the vertices $s \in \partial\tilde{E}$, i.e. $\Delta\tilde{x}_s = \sum_{e \in \delta_s} \tilde{x}_e$ for each $s \in \partial\tilde{E}$. Following Ref [15], we call $\Delta\tilde{x}$ the *syndrome* of \tilde{x} . Then define $E_0(\tilde{E}, u) \subset E_0(\tilde{E}, \partial\tilde{E})$ to be the set $E_0(\tilde{E}, u) := \{\tilde{x} \in E_0(\tilde{E}, \partial\tilde{E}) : (\Delta\tilde{x})_s = u_s \ \forall s \in \partial\tilde{E}\}$, where $u = u_1 \dots u_{|\partial\tilde{E}|}$ is a given syndrome.

Lemma V.3 $E_0(\tilde{E}, \partial\tilde{E}) = \bigcup_{u \in S} E_0(\tilde{E}, u)$ where S is the set of all bitstrings over the vertices in $\partial\tilde{E}$ that have an even number of 1's.

Proof Since every $\tilde{x} \in E_0(\tilde{E}, \partial\tilde{E})$ has some parity $\partial\tilde{x}$ on the vertices in $\partial\tilde{E}$, it is immediate that $E_0(\tilde{E}, \partial\tilde{E}) = \bigcup_{u \in \mathbf{u}} E_0(\tilde{E}, u)$ for some set \mathbf{u} of bitstrings over the vertices in $\partial\tilde{E}$. We only need to show that $\mathbf{u} = S$. Indeed, $E_0(\tilde{E}, u)$ is defined by the $|\tilde{V}|$ equations: $\sum_{e \in \delta_s} \tilde{x}_e = 0$ for all $s \in \tilde{V} \setminus \partial\tilde{E}$, and $\sum_{e \in \delta_s} \tilde{x}_e = u_s$ for all $s \in \partial\tilde{E}$. If we add together these equations for all $s \in \tilde{V}$, we obtain: $0 = \sum_{s \in \partial\tilde{E}} u_s$. Thus the equations defining $E_0(\tilde{E}, u)$ are inconsistent if $u \notin S$. On the other hand, there are no further linear dependencies among the equations, so $E_0(\tilde{E}, u) \neq \emptyset$ if $u \in S(\tilde{E})$. Since $E_0(\tilde{E}, u) \cap E_0(\tilde{E}, u') = \emptyset$ for any $u, u' \in S$ such that $u \neq u'$, it follows that \mathbf{u} cannot be a proper subset of S . \square

Corollary V.4 $|E_0(\tilde{E}, u)| = 2^{|\tilde{E}| - |\tilde{V}| + 1}$ for all $u \in S(\tilde{E})$ (and similarly for \hat{E}).

Proof The above considerations imply that $E_0(\tilde{E}, u)$ has the same size for each $u \in S(\tilde{E})$ and so $|E_0(\tilde{E}, \partial\tilde{E})| = |S(\tilde{E})| |E_0(\tilde{E}, u)|$. From its definition, $|S(\tilde{E})| = 2^{|\partial\tilde{E}| - |\tilde{n}|}$, while $|E_0(\tilde{E}, \partial\tilde{E})|$ is given by Lemma V.2. \square

Corollary V.5 For any $u \in S(\tilde{E})$, $E_0(\tilde{E}, u) = \tilde{z}(u) \oplus E_0(\tilde{E})$ where $\tilde{z}(u)$ is any fixed member of the set $E_0(\tilde{E}, u)$.

Proof For any $\tilde{x} \in E_0(\tilde{E})$ and $\tilde{z}(u) \in E_0(\tilde{E}, u)$, $\tilde{x} \oplus \tilde{z}(u) \in E_0(\tilde{E})$, since $\Delta(\tilde{x} \oplus \tilde{z}(u)) = \Delta\tilde{x} \oplus \Delta\tilde{z}(u) = u$. Thus, $\tilde{z}(u) \oplus E_0(\tilde{E}) \subseteq E_0(\tilde{E}, u)$. Furthermore, $|\tilde{z}(u) \oplus E_0(\tilde{E})| = |E_0(\tilde{E}, u)|$, so $E_0(\tilde{E}, u) = \tilde{z}(u) \oplus E_0(\tilde{E})$. \square

Note that all of the above considerations apply to the edge set \hat{E} as well. We are now in a position to construct a Schmidt decomposition of the state $|\bar{\tau}\rangle$ with respect to the (\tilde{E}, \hat{E}) bipartition of qubits.

Theorem V.6 A Schmidt decomposition of $|\bar{\tau}\rangle$ is

$$|\bar{\tau}\rangle = \frac{1}{\sqrt{2^{|\partial\tilde{E}| - 1}}} \sum_{u \in S} |K_{\tilde{E}}(u)\rangle \otimes |K_{\hat{E}}(u)\rangle, \quad (17)$$

where

$$|K_{\tilde{E}}(u)\rangle := \frac{1}{\sqrt{|E_0(\tilde{E}, u)|}} \sum_{\tilde{x} \in E_0(\tilde{E}, u)} |\tilde{x}\rangle$$

and $|K_{\hat{E}}(u)\rangle$ is defined analogously.

Proof Note first that

$$E_0(G) = \{(\tilde{x}, \hat{x}) \in E_0(\tilde{E}, \partial\tilde{E}) \otimes E_0(\hat{E}, \partial\hat{E}) : \partial\tilde{x} = \partial\hat{x}\}.$$

Then, by Lemma V.3:

$$|\bar{+}\rangle = \frac{1}{\sqrt{|E_0(G)|}} \sum_{\tilde{u}, \hat{u} \in S} \sum_{\tilde{x} \in E_0(\tilde{E}, \tilde{u})} \sum_{\hat{x} \in E_0(\hat{E}, \hat{u})} \delta_{\tilde{u}, \hat{u}} |\tilde{x}\rangle |\hat{x}\rangle. \quad (18)$$

Equation 17 now follows by the definition of S and working out the normalizations using Corollary V.4. It is easy to see that $\langle K_{\tilde{E}}(u') | K_{\tilde{E}}(u) \rangle = \delta_{u, u'}$, and similarly for \hat{E} . \square

The reduced density matrix on the subsystem of qubits corresponding to the edges in \tilde{E} is then, by Equation 17:

$$\rho_{\tilde{E}} = \text{tr}_{e \in \hat{E}} (|\bar{+}\rangle \langle \bar{+}|) = \frac{1}{2^{|\partial\tilde{E}|-1}} \sum_{u \in S} |K_{\tilde{E}}(u)\rangle \langle K_{\tilde{E}}(u)|. \quad (19)$$

We note that it is evident from the normalization in Equation 19 that $|\bar{+}\rangle$ obeys the so-called *entanglement area law*: the entropy of entanglement of a block of spins grows linearly with the size of its perimeter.

For an arbitrary surface-code state $|\bar{\psi}\rangle = \sum_{\gamma \in \{0,1\}^{\otimes 2g}} c_\gamma |\bar{X}_\gamma\rangle$, define $\rho_{\tilde{E}}(|\bar{\psi}\rangle) := \text{tr}_{e \in \hat{E}} (|\bar{\psi}\rangle \langle \bar{\psi}|)$. Then using Equation 17 we have

$$\rho_{\tilde{E}}(|\bar{\psi}\rangle) = \frac{1}{2^{|\partial\tilde{E}|-1}} \sum_{u, u' \in S} \sum_{\gamma, \delta} c_\gamma c_\delta^* \bar{Z}_{\tilde{E}}^\gamma |K_{\tilde{E}}(u)\rangle \langle K_{\tilde{E}}(u')| \bar{Z}_{\tilde{E}}^\delta \langle K_{\tilde{E}}(u') | \bar{Z}_{\tilde{E}}^{\gamma \oplus \delta} |K_{\tilde{E}}(u)\rangle, \quad (20)$$

where $\bar{Z}_{\tilde{E}}^\gamma := \prod_{j=1}^{2g} (\prod_{e \in C'_j \cap \tilde{E}} Z_e)^{\gamma_j}$ and analogously for \hat{E} . We can evaluate the matrix product using the definition of $|K_{\tilde{E}}(u)\rangle$:

$$\begin{aligned} \langle K_{\hat{E}}(u') | \bar{Z}_{\hat{E}}^{\gamma \oplus \delta} |K_{\hat{E}}(u)\rangle &= \frac{1}{|E_0(\hat{E}, u)|} \sum_{\hat{x}, \hat{y} \in E_0(\hat{E}, u)} \langle \hat{y} | \bar{Z}_{\hat{E}}^{\gamma \oplus \delta} | \hat{x} \rangle \\ &= \frac{\delta_{u, u'}}{|E_0(\hat{E}, u)|} \prod_{j=1}^{2g} (-1)^{(\gamma \oplus \delta)_j |\hat{z}(u) \cap C'_j|} \\ &\quad \sum_{\hat{x} \in E_0(\hat{E})} \prod_{j=1}^{2g} (-1)^{(\gamma \oplus \delta)_j |\hat{x} \cap C'_j|}, \end{aligned} \quad (21)$$

where $\hat{z}(u)$ is any fixed member of the set $E_0(\hat{E}, u)$ and we have used Corollary V.5 in the last step. Consider any value of j such that $(\gamma \oplus \delta)_j = 1$. If there exists any $\hat{y} \in E_0(\hat{E})$ such that $|\hat{y} \cap C'_j| = 1 \pmod{2}$, then the above

summation over $\hat{x} \in E_0(\hat{E})$ vanishes. That is because for each $\hat{x} \in E_0(\hat{E})$, the bitstring $\hat{x} \oplus \hat{y}$ term will have the opposite sign as the \hat{x} term and the two will cancel, since $|\hat{x} \oplus \hat{y} \cap C'_j| = 1 + |\hat{x} \cap C'_j|$. Let A denote the set of $j \in \{1 \dots 2g\}$ such that there exists a $\hat{y} \in E_0(\hat{E})$ satisfying $|\hat{y} \cap C'_j| = 1 \pmod{2}$. Let B denote the set of j that are not in A , but for which $C'_j \cap \hat{E} \neq \emptyset$. So we can rewrite the RHS of Equation 21 as

$$\delta_{u, u'} \prod_{j \in A} \delta_{\gamma_j, \delta_j} \prod_{j \in B} (-1)^{(\gamma \oplus \delta)_j |\hat{z}(u) \cap C'_j|}$$

because if $\gamma_j = \delta_j$ for all $j \in B$ then each term in the summation over $\hat{x} \in E_0(\hat{E})$ is positive, cancelling the overall factor of $|E_0(\hat{E}, u)|^{-1}$. Using this and Equation 20, we can now consider a partial measurement probability for the qubits in \tilde{E} :

$$\begin{aligned} p(|\phi_{\tilde{E}}\rangle) &= \langle \phi_{\tilde{E}} | \rho_{\tilde{E}}(|\bar{\psi}\rangle) | \phi_{\tilde{E}} \rangle \\ &= \frac{1}{2^{|\partial\tilde{E}|-1}} \sum_{\gamma, \delta} c_\gamma c_\delta^* \prod_{j \in A} \delta_{\gamma_j, \delta_j} \langle \phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^* | \bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta \\ &\quad \sum_{u \in S} (-1)^{\sum_{j \in B} (\gamma \oplus \delta)_j |\hat{z}(u) \cap C'_j|} |K_{\tilde{E}}(u) \otimes K_{\tilde{E}}(u)\rangle. \end{aligned} \quad (22)$$

In this notation, we have replaced the product of two matrix elements $\langle \phi_{\tilde{E}} | \bar{Z}_{\tilde{E}}^\gamma | K_{\tilde{E}}(u) \rangle \langle K_{\tilde{E}}(u') | \bar{Z}_{\tilde{E}}^\delta | \phi_{\tilde{E}} \rangle$ in the Hilbert space of $|\tilde{E}|$ qubits with a single matrix element $\langle \phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^* | \bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta | K_{\tilde{E}}(u) \otimes K_{\tilde{E}}(u') \rangle$ in the Hilbert space of $2|\tilde{E}|$ qubits. Here $|\phi_{\tilde{E}}^*\rangle$ is a product state obtained from $|\phi_{\tilde{E}}\rangle$ by complex conjugating a_e and b_e for each $e \in \tilde{E}$. $\bar{Z}_{\tilde{E}_1}^\gamma$ is the operator $\bar{Z}_{\tilde{E}}^\gamma$ applied to the first copy of \tilde{E} , denoted as \tilde{E}_1 (and likewise for \tilde{E}_2).

Equation 21 relates $p(|\phi_{\tilde{E}}\rangle)$ to a summation over states in the Hilbert space of a surface code on the graph $G(\tilde{E}_1) \cup G(\tilde{E}_2)$, defined by taking two copies of $G(\tilde{E})$ and gluing them together at the vertices in the boundary $\partial\tilde{E}$ (as in [15]). When the set B is empty for example, the ket in Equation 21 becomes $\sum_{u \in S} |K_{\tilde{E}}(u) \otimes K_{\tilde{E}}(u)\rangle$, which is the logical $+1$ X eigenstate $|\bar{+}\rangle$ of the surface code on $G(\tilde{E}_1) \cup G(\tilde{E}_2)$. This is because the set of cycles $E_0(G(\tilde{E}_1) \cup G(\tilde{E}_2))$ on this graph has the structure: $E_0(G(\tilde{E}_1) \cup G(\tilde{E}_2)) = \{(\tilde{x}, \tilde{y}) \in E_0(\tilde{E}, \partial\tilde{E}) \otimes E_0(\tilde{E}, \partial\tilde{E}) : \partial\tilde{x} = \partial\tilde{y}\}$. In the notation of Equation 1:

$$|K(G(\tilde{E}_1) \cup G(\tilde{E}_2))\rangle = \frac{1}{\sqrt{2^{|\partial\tilde{E}|-1}}} \sum_{u \in S} |K_{\tilde{E}}(u) \otimes K_{\tilde{E}}(u)\rangle.$$

B. MBQC on punctured cylinder graphs

We now define the family of punctured cylinder graphs and apply the above analysis to them. To construct a cellularly embedded punctured cylinder graph, consider an

$N \times M$ square lattice with periodic boundary conditions in the vertical direction, embedded on the surface of a solid disk. Then, imagine drilling g thin holes (or “slots”) through the disk, each one in between two rows of vertices on the graph. Finally, vertical edges are extended through each slot, as in Figure 6 below.

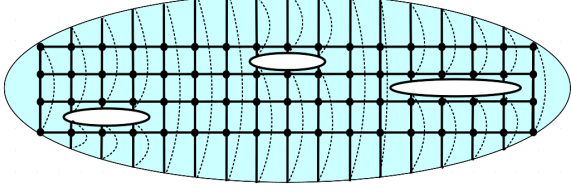


FIG. 6: (Color online) A three-slot punctured cylinder graph cellularly embedded on a surface of genus three.

A family of such punctured cylinder graphs is parameterized by the dimensions of the lattice along with the position and width of each slot: $\{N, M, \{x_1, y_1, K_1\}, \dots, \{x_g, y_g, K_g\}\}$. We will take the slots to be ordered from left to right ($x_{j+1} > x_j$), and assume that no two slots are above one another ($x_{j+1} \geq x_j + K_j$). A flattened representation of a punctured cylinder graph is shown in Figure 7.

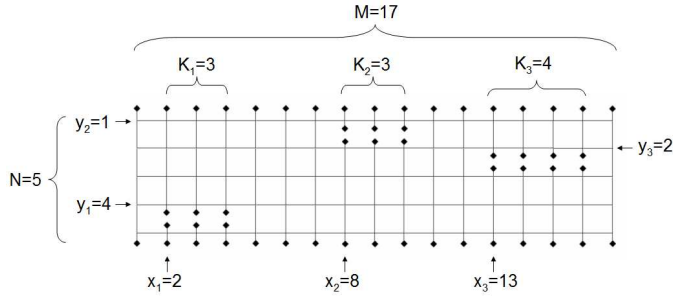


FIG. 7: A three-slot punctured torus graph. The $n = 3$ handles have positions (x_j, y_j) and widths K_j for $j = 1 \dots n$. Pairs of points marked by diamonds are identified within each column, according to Figure 6.

It will be necessary to give a concrete set of encoding cocycles C'_k for the punctured cylinder surface code. A suitable choice is shown in Figure 8. These cocycles in fact constitute a canonical encoding scheme (as defined in Appendix A). This is because one can continuously deform the loops drawn in Figure 8 for the cocycles C'_k such that they form a canonical polygonal schema (this does not change the edge sets E_k defined in Appendix A). This deformation is shown in Figure 10 for the simple case of a double torus.

We will also assume a particular order in which to make the single qubit measurements of MBQC on the punctured cylinder lattice, in order to simplify the analysis. Since the punctured cylinder graph has a left and right boundary, we may unambiguously start at the leftmost column, and measure the qubits column by column proceeding to the right. That is: first we measure all qubits

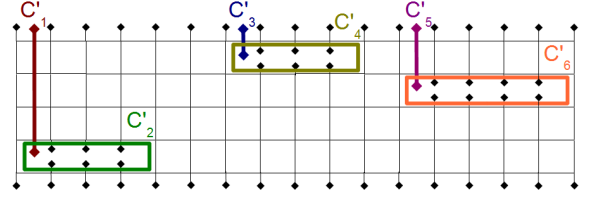


FIG. 8: (Color online) A set of 6 non-trivial cocycles C'_k on a three-slot punctured cylinder graph. The edges included in a cocycle are those that are crossed by the line depicted.

on the vertical edges in column 1, then all of the qubits on horizontal edges between columns 1 and 2, then the vertical edge qubits in column 2, and so on. We further take the measurements to occur row by row as one moves down a column of horizontal or vertical edges. For brevity, we will call this ordering of measurements **LtoR**. **LtoR** seems to be a natural choice because it mimics the simple temporal order in a quantum circuit, and it satisfies the assumption of the previous section that both \tilde{E} and \hat{E} are connected at all stages.

Our main result of this section is the following theorem:

Theorem V.7 Consider a state $|\bar{\psi}\rangle$ in the surface-code space of a punctured cylinder graph G of genus g . For MBQC on $|\bar{\psi}\rangle$ with the measurement ordering **LtoR**, at any step \tilde{E} of computation and for product state of outcomes $|\phi_{\tilde{E}}\rangle$:

$$p(|\phi_{\tilde{E}}\rangle) = \alpha \langle \phi(G'(\tilde{E})) | \bar{\psi}(G'(\tilde{E})) \rangle,$$

where $G'(\tilde{E})$ is an embedded punctured cylinder graph of genus less than or equal to $2g$, $|\bar{\psi}(G'(\tilde{E}))\rangle$ is a state in the codespace of $G'(\tilde{E})$, $|\phi(G'(\tilde{E}))\rangle$ is a product state, and α is a known proportionality.

Proof See Appendix C.

Together with Theorem IV.2, we then have the following Corollary:

Corollary V.8 For MBQC with the measurement scheme **LtoR** on a punctured cylinder code state $|\bar{\psi}\rangle$, if an optimal local basis for the effective state $|\Phi\rangle$ corresponding to the inner product in Theorem V.7 is known at each step \tilde{E} of computation, then the probability distribution P over the outcomes of the next measurement can be classically sampled from in $\text{poly}(|E|, g) 2^{E_{\text{Sch}}(|\Phi\rangle)}$ steps.

As a special case of Theorem V.8, MBQC on the states $|\bar{C}^{\alpha, \beta}\rangle$ in the codespace of the punctured cylinder code can be simulated completely efficiently in the strong sense of sampling:

Theorem V.9 The probability distribution P of computational output values of MBQC on one of the states

$|\bar{C}^{\alpha,\beta}\rangle$ in the code space of the punctured cylinder code (with the measurement scheme **LtoR**) can be sampled from efficiently in both $|E|$ and g .

Proof See Appendix D.

VI. CONCLUSION

We have considered the classical simulation of MBQC with surface-code states as resource states. We first showed that for surface-code states the probability of obtaining any single MBQC outcome can be computed in a number of steps that scales polynomially in the size of the surface-code embedded graph, and at worst exponentially in its genus. We found a family of states in the code space of any surface code for which this probability can be computed efficiently in both the size and the genus of the graph. For intermediate cases, we found a connection between the complexity of computing such probabilities and entanglement. In particular, the cost scales exponentially in the Schmidt measure of a state which combines the specification of MBQC outcomes and the quantum state being encoded into the surface code. We also considered the task of sampling from the probability distribution over MBQC outcomes, and saw that for MBQC on a certain family of embedded graphs with a simple ordering of measurements, this task is equivalent to computing a single MBQC outcome probability for a modified graph. From this we were able to define a class of higher genus surface-code states for which MBQC can be efficiently classically simulated.

Acknowledgments

We are thankful to Pradeep Sarvepalli and Shuhang Yang for useful discussions. This work is supported by NSERC, CIFAR, Mprime and IARPA.

Appendix A: Evaluating the Generating Function of Cycles

In this Appendix we show that the generating function of cycles on an embedded graph G can be written in the form of Equation 8:

$$\text{Cy}(G, w) = \frac{1}{2^g} \sum_{\alpha, \beta \in \{0,1\}^{\otimes g}} (-1)^{\alpha \cdot \beta} \text{Pf}(\mathcal{A}'(w^{\alpha, \beta})).$$

To arrive at Equation 8, we map the problem of evaluating the generating function of cycles on G to the problem of evaluating the generating function of perfect matchings on a modified graph G' . Then we apply a result from [32] to evaluate this generating function.

A *perfect matching* M of a graph G is a subset of the edges of G such that every vertex contains exactly one

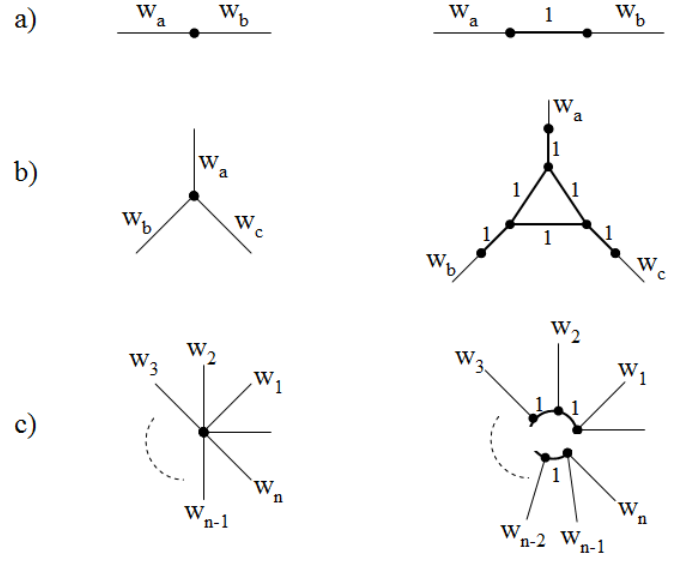


FIG. 9: Transformations at each vertex from G to a modified graph G' .

edge incident upon it in M . Let $\mathcal{PM}(G)$ denote the set of all perfect matchings on G . If to each edge e we associate a weight w_e , then the generating function of perfect matchings on G is defined as

$$P(G, w) := \sum_{M \in \mathcal{PM}(G)} \prod_{e \in M} w_e.$$

We now define a modified embedded graph G' by the following four rules, adapted from [26] and [33]:

- If any vertex v has exactly one edge incident upon it, remove it and the incident edge from G
- For any vertex v with exactly two edges a and b incident upon it, split v into two vertices connected by a new edge with weight 1, as shown in Figure 9a.
- For any vertex v with exactly three edges incident upon it, replace v with six vertices and nine edges as shown in Figure 9b.
- For any vertex with $n > 3$ edges incident upon it, first replace v with $n - 1$ vertices of degree three as shown in Figure 9c, and then follow the rule for a degree three vertex for each of the resulting vertices.

The above rules define a graph G' which differs from G only locally around each vertex (and deletion of vertices of degree one). Thus, it also has a natural embedding on S where the modification around each vertex can be made arbitrary small. Furthermore, it can be verified that there exists a one-to-one mapping between cycles $x \in E_0(G)$ on G and perfect matchings $M \in \mathcal{PM}(G')$ on

G' , and that the product of edge weights for a given cycle on G is equal to that of the associated perfect matching on G' . So:

$$\text{Cy}(G, w) = P(G', w'),$$

where w' denotes the edge weights w_e for all $e \in E$ along with $w_e = 1$ for all of the new edges introduced in the transformation $G \rightarrow G'$.

In [32], Galluccio and Loebl study the problem of evaluating the generating function of perfect matchings on a graph G' that is embedded on an orientable surface of genus g . Their main result (Theorem 3.9 of [32]) is a formula for $P(G', w)$ that can be written in the form of Equation 8. Therein the function $\text{Pf}(\mathcal{A}'(w^{\alpha, \beta}))$ is the Pfaffian of a $|V'| \times |V'|$ weighted adjacency matrix $\mathcal{A}'(w^{\alpha, \beta})$, where $|V'|$ is the number of vertices in the graph G' (a few more edges may need to be added to G' , as we shall see at the end of this section). The Pfaffian $\text{Pf}(M)$ of a $2N \times 2N$ matrix M is a polynomial in the matrix entries that is related to the determinant, and can be computed in $\text{poly}(N)$ time. In their work, Galluccio and Loebl take the embedded graph as being specified by a so-called *canonical polygonal schema*. A *curve* in S is a continuous map $h : [0, 1] \rightarrow S$, and a *loop* is a curve with $h(1) = h(0)$. A canonical polygonal schema of a graph G is obtained from its embedding on S by cutting S along $2g$ loops $\mathcal{C}_1 \dots \mathcal{C}_{2g}$, chosen such that after the cutting S can be unfolded into a convex polygon B_0 with $4g$ sides. Each cut \mathcal{C}_k produces two paired sides of B_0 , which we denote as \mathcal{C}_k^1 and \mathcal{C}_k^2 , and the sides of B_0 are arranged in clockwise order as $\mathcal{C}_1^1, \mathcal{C}_2^1, \mathcal{C}_1^2, \mathcal{C}_2^2, \mathcal{C}_3^1, \mathcal{C}_2^1, \mathcal{C}_3^2, \dots, \mathcal{C}_{2g}^1, \mathcal{C}_{2g}^2$. The closed surface S can be reconstructed by glueing \mathcal{C}_k^1 and \mathcal{C}_k^2 back together with the proper orientation.

To use the results of reference [32] then, we require a suitable set of loops $\mathcal{C}_1 \dots \mathcal{C}_{2g}$ on S . These can be chosen as follows: draw $2g$ non-self-intersecting curves on S that all begin and end at a common *base point* x , but are otherwise non-overlapping and non-crossing, and such that for each j : \mathcal{C}_{2j-1} goes around the j^{th} handle, and \mathcal{C}_{2j} goes through the j^{th} handle. See Figure 10b for an example. Consider now the original graph G embedded on S . Choose the basepoint to be at the center of some face f of G . Without loss of generality, we may choose the \mathcal{C}_k to avoid the vertices of G and cross the embeddings of the edges of e only at isolated points. After cutting S along these loops, we are left with a plane graph plus some cut edges. We define G_0 as the plane graph on B_0 consisting of all of the vertices of G and all of the edges that do not cross any of the cuts \mathcal{C}_k . Let E_k denote the set of edges of G that cross the loop \mathcal{C}_k an odd number of times. We now prove a few properties of the sets E_k .

Lemma A.1 *For each $k \in \{1 \dots 2g\}$, the edge set E_k is a cycle of G .*

Proof For each $f \in F$, the cycle ∂f defines a loop or set of disjoint loops \mathcal{C}_f on S . Since \mathcal{C}_f forms the boundary of a region of S , the loops \mathcal{C}_f and \mathcal{C}_k cross an even number

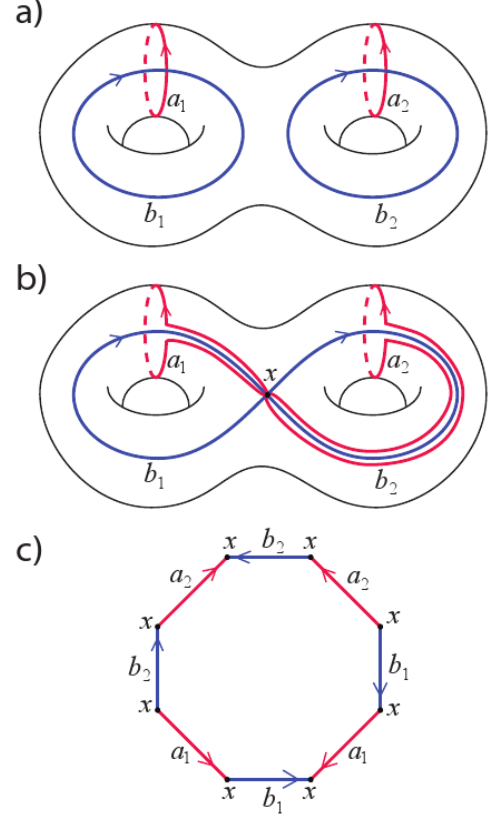


FIG. 10: (Color online) a) A set of loops on a double torus defining a set of punctured cylinder graph cocycles \mathcal{C}'_k as shown in Figure 8, b) a deformation of these loops to define a canonical polygonal schema, and c) the octagon obtained after cutting along the loops shown in b) and unfolding the surface. To visualize the move between Figures b) and c), one may separate the two tori and imagine unfolding each individually into a single torus with a boundary, as shown in Figure 84 of [34] (p.71).

of times (this follows from the Jordan Curve Theorem). So, there cannot be an odd number of edges $e \in \partial f$ that cross \mathcal{C}_k an odd number of times. Thus $|\partial f \cap E_k|$ is even for every face $f \in F$. \square

Lemma A.2 *The cocycles E_k are homologically independent on \tilde{G} .*

Proof If this were not true, then for some collection $Y \subseteq \{1 \dots 2g\}$ of the E_k and some set $\tilde{V} \subset V$ of vertices, we would have:

$$\bigoplus_{k \in Y} E_k = \bigoplus_{v \in \tilde{V}} \delta v.$$

The edge set $\bigoplus_{k \in Y} E_k$ is precisely the set of edges that are crossed an odd number of times by the loop \mathcal{C}_Y , which we define as the concatenation of the loops \mathcal{C}_k for all $k \in Y$, in some arbitrary order. By continuously deforming \mathcal{C}_Y around the vertices $v \in \tilde{V}$, one obtains a modified loop $\tilde{\mathcal{C}}_Y$ that crosses all edges $e \in E$ either an even number of

times or not at all. Removal of the loop \mathcal{C}_Y from S does not separate the surface, because cutting along *all* of the \mathcal{C}_k results in a single polygon B_0 , which is still connected. Since $\hat{\mathcal{C}}_Y$ is related to \mathcal{C}_Y by a continuous deformation, its removal does not separate S either. But now we can prove a contradiction, because a non-surface-separating loop must intersect at least one edge of G an odd number of times.

To demonstrate this, we use a result from [35] (cf. Lemma 3). First, we define an embedded graph \hat{G}_Y which combines the original graph G , and the loop $\hat{\mathcal{C}}_Y$ as follows. Add a vertex to G at each point where $\hat{\mathcal{C}}_Y$ crosses an edge of G , and a vertex at the base point x of the canonical polygonal schema. For each section of $\hat{\mathcal{C}}_Y$ between two intersection points with G , add an edge that traces the section. Finally, add edges that trace $\hat{\mathcal{C}}_Y$ between the basepoint x and the points where $\hat{\mathcal{C}}_Y$ first crosses an edge from x . The new edges that trace out the loop $\hat{\mathcal{C}}_Y$ define a cycle of \hat{G}_Y , which we denote as \hat{c}_Y . For any edge e of G that was split into several edges $e_1 \dots e_k$ by the transformation $G \rightarrow \hat{G}_Y$, let \hat{e} denote the set $\{e_1 \dots e_k\}$. The number of times that $\hat{\mathcal{C}}_Y$ crosses the edge e of G is then $|\hat{e}| - 1$. Let $\{Q_1 \dots Q_{2g}\}$ denote any set of $2g$ homologically independent cycles on G , and for each Q_j let \hat{Q}_j denote the corresponding cycle on \hat{G}_Y (simply let $\{e\} \rightarrow \hat{e}$ for any edge e that is crossed by $\hat{\mathcal{C}}_Y$). By Lemma 3 of [35], there exists some j such that \hat{Q}_j is crossed by \hat{c}_Y an odd number of times, iff \hat{c}_Y is a homologically non-trivial cycle on \hat{G}_Y . The cycle \hat{c}_Y must be homologically non-trivial on \hat{G}_Y , because if it were not then it would form the boundary of a set of faces of \hat{G}_Y , and cutting along \hat{c}_Y (or equivalently $\hat{\mathcal{C}}_Y$) would separate the surface S (a similar argument shows that the \hat{Q}_j are homologically independent on \hat{G}_Y , which is necessary for our use of the result in [35]). So \hat{c}_Y crosses \hat{Q}_j an odd number of times, for some j . But, if there were no edge e of G that was crossed an odd number of times by $\hat{\mathcal{C}}_Y$, then \hat{Q}_j and \hat{c}_Y could only cross an even number of times (or zero). So there does exist such an edge e . \square

Theorem A.3 *The cocycles E_k constitute a possible choice of encoding cocycles C'_k for the surface code on G .*

Proof By Lemma A.2, the cocycles E_k are homologically independent on \tilde{G} . All that's left is to show that with encoded \mathbb{Z} cocycles defined as $C'_k := E_k$, there exists at least one set of encoding cycles for the X operators C_k on G such that $|C_j \cap C'_k| = \delta_{jk} \pmod{2}$. As discussed in Section II, a tree-cotree decomposition of G guarantees the existence of homologically independent cycles $T(e_1) \dots T(e_{2g})$ and homologically independent cocycles $C(e_k) \dots C(e_{2g})$ on G such that $|T(e_j) \cap C(e_k)| = \delta_{jk}$. The cocycles $C(e_k)$ along with the edge sets δ_v for all $v \in V$ form a basis for all cocycles on G with respect to the symmetric difference of sets. So, $C'_k = \bigoplus_{m \in Y_k} C(e_m) \oplus \bigoplus_{v \in V_k} \delta_v$ for some $Y_k \subseteq \{1 \dots 2g\}$ and $V_k \subseteq V$. Since the C'_k are homologically independent, the $2g \times 2g$ matrix A defined by

$A_{mk} \in \{0, 1\} : A_{mk} = 1$ iff $m \in Y_k$ is invertible over the binary field \mathbb{Z}_2 . Let A^{-1} denote its \mathbb{Z}_2 inverse and define the set Y_j^{-1} as the set of all l for which $A_{jl}^{-1} = 1$. Then define a set of encoding cycles as $C_j := \bigoplus_{l \in Y_j^{-1}} T(e_l)$. Using the definition of a cycle and $|T(e_l) \cap C(e_m)| = \delta_{lm}$

$$|C_j \cap C'_k| = \bigoplus_{l \in Y_j^{-1}} \bigoplus_{m \in Y_k} \delta_{lm} = \bigoplus_{m=1}^{2g} A_{jm}^{-1} A_{mk} = \delta_{jk},$$

where in this expression \bigoplus denotes mod 2 addition of numbers. Finally, the cycles C_j so defined are homologically independent on G because the matrix A^{-1} is invertible over \mathbb{Z}_2 . \square

Definition A.4 *Given a canonical polygonal schema $\{\mathcal{C}_k\}$, a canonical encoding scheme is the choice of encoding cocycles $C'_k := E_k$. This is a valid one by Theorem A.3.*

So far, we've defined a canonical polygonal schema $\{\mathcal{C}_k\}$ for S , and the associated canonical encoding scheme $\{E_k\}$ for the surface code of G . We now apply these concepts to the modified graph G' . Since all of the vertices of G belong to the interior of B_0 , we can perform the graph modification $G \rightarrow G'$ in an arbitrarily small neighborhood of each vertex *after* unfolding the embedded graph G . We take the \mathcal{C}_k to be chosen such that they avoid crossing any edge e that is incident on a vertex of degree one (one may merely drag \mathcal{C}_k across that vertex to avoid e). This yields a canonical polygonal schema for G' , where the edge set E_k is still the set of edges of G' that cross the cut \mathcal{C}_k an odd number of times.

Another modification of the graph G' is necessary for us to use Equation 8 (see Corollary 3.9 of [32]). Consider any edge e that crosses n possibly non-distinct cuts $\mathcal{C}_{k_1} \dots \mathcal{C}_{k_n}$, in that order as you follow e in one direction. If $n > 1$, then one modifies G' by adding $2n$ vertices and replacing e by a string of edges $e_1 \dots e_{2n+1}$ connected in a chain such that e_{2j-1} crosses one cut \mathcal{C}_{k_j} for each $j = 1 \dots n$. Edge e_1 is given weight w_e while the rest of the edges receive a weight of $w_{e_j} = 1$. Call this transformation *bridge splitting*. Bridge splitting guarantees that no edge of G' crosses more than one cut, or any single cut more than once. Let E'_k denote the set of edges of G' that cross the cut \mathcal{C}_k . Let w' continue to denote the set of weights of the edges of G' . One may verify that the generating function $P(G', w')$ of perfect matchings is unchanged by bridge splitting. After bridge splitting, a few more minor transformations of the graph may be necessary (see [32]), but these do not affect our analysis.

Now we consider the construction of the weighted adjacency matrices $\mathcal{A}'(w^{\alpha, \beta})$ in Equation 8. Let G'_0 be the subgraph of G' that belongs entirely to B_0 . G'_0 contains all of the vertices of G' , and all of the edges that do not cross any cut. An *orientation* of a graph is an assignment of a direction to each edge. As a plane graph, it can be shown that G'_0 has an orientation D_0 of its

edges such that the boundary of each face has an odd number of edges oriented clockwise [36]. Such an orientation is called a *basic* orientation, and we fix a particular one D_0 . For each $k \in \{1 \dots 2g\}$, Galluccio and Loeb show that $G'_0 \cup E'_k$ has a natural plane embedding, and a unique orientation D_k of the edges E_k such that (D_0, D_k) is a basic orientation in this plane embedding. For any $\alpha, \beta \in \{0, 1\}^{\otimes 2g}$, a so-called *relevant orientation* of G' is defined as follows: start with the orientation $(D_0, D_1, D_2 \dots D_{2g})$, and reverse the orientation of all edges in E'_{2k-1} if $\alpha_k = 1$, and reverse the orientation of all edges E'_{2k} if $\beta_k = 1$, for each $k = 1 \dots g$. For any two vertices u, v of G' , we define the matrix element $[A'(w')^{\alpha, \beta}]_{u, v}$ to be 0 if u and v are not connected by an edge, w'_e if u and v are connected by an edge e oriented from u to v , and $-w'_e$ if u and v are connected by an edge e oriented from v to u , where the edge orientations are defined by the relevant orientation α, β .

The matrix $A'(w')^{\alpha, \beta}$ depends both on α and β and the edge weights w'_e . Reversing the orientation of an edge has the same effect as multiplying the corresponding edge weight by -1 . So, we may write $A'(w')^{\alpha, \beta} = A'(w'^{\alpha, \beta})$ where $A'(w')$ denotes the adjacency matrix $A'(w')^{0, 0}$ of G' corresponding to the concatenation of the basic orientations $(D_0, D_1, D_2 \dots D_{2g})$, and $w'^{\alpha, \beta}$ is the set of edge weights w' after we multiply by -1 all edge weights along the cocycle E'_{2k-1} if $\alpha_k = 1$ and along the cocycle E'_{2k} if $\beta_k = 1$. Recall that the edge weights w' of G' are determined by the edge weights w of G , so we could denote $A'(w')$ as $\mathcal{A}'(w)$, where the matrix $\mathcal{A}'(\cdot)$ incorporates the effect of the graph modifications $G \rightarrow G'$. We will now show that $\text{Pf}(A'(w')^{\alpha, \beta}) = \text{Pf}(\mathcal{A}'(w^{\alpha, \beta}))$, where $w^{\alpha, \beta}$ is the set of edge weights w of G after we multiply by -1 the edge weight w_e once for each time it belongs to a cocycle E_{2k-1} for which $\alpha_k = 1$, and once for each time it belongs to a cocycle E_{2k} for which $\beta_k = 1$. Each nonzero term of the Pfaffian $\text{Pf}(A'(w')^{\alpha, \beta})$ depends on w' only via the product of edge weights $w'^{\alpha, \beta}_e$ for the edges e in a particular perfect matching of G' (see Definition 1.3 in [32]). For any edge $e \in E$ that was replaced by a set of edges $e_1 \dots e_{2n+1}$ during the bridge splitting process, a perfect matching of G' contains either none or all of $\{e_1, e_3 \dots e_{2n+1}\}$. If $e \in E_k$, then there are an odd number of e_{2j-1} that cross the cut \mathcal{C}_k . Multiplying the weights of all of these edges by -1 yields an overall minus sign for a term containing $\{e_1, e_3 \dots e_{2n+1}\}$, which has the exact same effect as letting $w_e \rightarrow -w_e$ before bridge splitting. If on the other hand e crosses \mathcal{C}_k but an even number of times, then there are an even number of e_{2j-1} that cross the cut \mathcal{C}_k , and there is no effect on $\text{Pf}(A'(w')^{\alpha, \beta})$ from multiplying the weights of these edges by -1 . Finally, with $\text{Pf}(A'(w')^{\alpha, \beta}) = \text{Pf}(\mathcal{A}'(w^{\alpha, \beta}))$, Equation 8 holds up to a possible overall minus sign by Theorem 3.9 of [32]. The possible minus sign depends upon D_0 and the structure of the graph G' , but not on the edge weights $w^{\alpha, \beta}$. So we may neglect it as it would only add an overall phase to $\langle \psi | \phi \rangle$ in Equation 7.

Appendix B: Proof of Theorem IV.3

We will show that under the assumptions of the theorem, if

$$|\Phi\rangle = \sum_{j=1}^s |\chi_1^j\rangle |\chi_2^j\rangle \dots |\chi_{|E|}^j\rangle$$

for any set of single qubit states $|\chi_k^j\rangle$, then $s \geq D$. Our first step will be to isolate a single term of Equation 16 by taking a partial inner product between $|\Phi\rangle$ and a particular state on the qubits in \mathbf{A} .

In the following, the distinction between the even and odd numbered cocycles will not be important, so we simplify notation by writing the coefficients $\Psi_{\alpha, \beta}$ as Ψ_α where α is now a $2g$ component bitstring. Then we can rewrite Equation 16 as:

$$\begin{aligned} |\Phi\rangle &= \sum_{\alpha \in \{0, 1\}^{\otimes 2g}} \Psi_\alpha \left(\prod_{k=1}^{2g} \prod_{e \in C'_k} Z_e^{\alpha_k} \right) \bigotimes_{e \in E} |\phi_e\rangle \\ &= \sum_{\alpha \in \{0, 1\}^{\otimes 2g}} \Psi_\alpha \bigotimes_{e \in E} (Z_e)^{[M\alpha]_e} |\phi_e\rangle, \end{aligned}$$

where M is the $|E| \times 2g$ matrix such that $M_{e, k} = 1$ if $e \in C'_k$ and $M_{e, k} = 0$ if $e \notin C'_k$, for all $e \in E$. $[M\alpha]_e := \sum_{k=1}^{2g} M_{e, k} \alpha_k$.

Write $|\phi_e\rangle = a_e|0\rangle + b_e|1\rangle$ for any edge e . Now we define $|\phi_e^{0, \perp}\rangle := b_e^*|0\rangle + a_e^*|1\rangle$, and $|\phi_e^{1, \perp}\rangle := b_e^*|0\rangle - a_e^*|1\rangle$. It is easy to verify that for any edge e and binary variable $\gamma_k \in \{0, 1\}$

$$\langle \phi_e^{\gamma_k, \perp} | (Z_e)^{\alpha_k} | \phi_e \rangle = \delta_{\alpha_k, \gamma_k} 2a_e b_e.$$

In particular, $|\phi_e^{1, \perp}\rangle$ is perpendicular to $|\phi_e\rangle$ for any edge e , while $|\phi_e^{0, \perp}\rangle$ is perpendicular to $Z_e|\phi_e\rangle$ for any edge e . First we write Equation 16 in the form

$$|\Phi\rangle = \sum_{\alpha \in \{0, 1\}^{\otimes 2g}} \Psi_\alpha |\phi_{rest}^\alpha\rangle \otimes |\phi_{\mathbf{A}}^\alpha\rangle \otimes |\phi_{\mathbf{B}}^\alpha\rangle, \quad (\text{B1})$$

where $|\phi_{rest}^\alpha\rangle$ is a α -dependent product state on all of the qubits in the complement of $\mathbf{A} \cup \mathbf{B}$ in E , and

$$|\phi_{\mathbf{A}}^\alpha\rangle := \bigotimes_{k=1}^{2g} (Z_{e_k})^{[M\alpha]_{e_k}} |\phi_{e_k}\rangle = \bigotimes_{k=1}^{2g} (Z_{e_k})^{[M\mathbf{A}\alpha]_k} |\phi_{e_k}\rangle.$$

The states $|\phi_{e_k}^{\gamma_k, \perp}\rangle$ for any $2g$ component bitstring γ can now be used to pick out a single term in Equation B1, because

$$\left(\bigotimes_{k=1}^{2g} \langle \phi_{e_k}^{\gamma_k, \perp} | \right) |\phi_{\mathbf{A}}^\alpha\rangle = \left(\prod_{k=1}^{2g} 2a_{e_k} b_{e_k} \right) \delta_{\gamma, [M\mathbf{A}\alpha]}$$

and thus

$$\left(\bigotimes_{k=1}^{2g} \langle \phi_{e_k}^{[M\mathbf{A}\gamma]_k, \perp} | \right) |\Phi\rangle = \Psi_\gamma \left(\prod_{k=1}^{2g} 2a_{e_k} b_{e_k} \right) |\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle. \quad (\text{B2})$$

The only value of α for which $[M_{\mathbf{A}}\alpha] = [M_{\mathbf{A}}\gamma]$ is $\alpha = \gamma$, because by assumption the square matrix $M_{\mathbf{A}}$ has full rank and hence is invertible. Since $|\phi_{e_k}\rangle$ is not a Z-eigenstate, $2a_{e_k}b_{e_k}$ is nonzero for each k . We can show that the states $\{|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle\}$ for various bitstrings γ are a linearly independent family of states. This follows from the assumption of the second set \mathbf{B} of non-Z eigenstate edges $\{e'_k\}$ for which $M_{\mathbf{B}}$ has full rank. For we can repeat the above trick to show that each $|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle$ has a component that is perpendicular to subspace spanned by the rest of the $|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle$:

$$\left(\langle \phi_{rest}^\gamma | \otimes \bigotimes_{k=1}^{2g} \langle \phi_{e'_k}^{[M_{\mathbf{B}}\gamma]_{k,\perp}} | \right) |\phi_{rest}^\alpha\rangle \otimes |\phi_{\mathbf{B}}^\alpha\rangle \begin{cases} = 0 & : \alpha \neq \gamma \\ \neq 0 & : \alpha = \gamma \end{cases}.$$

The RHS is zero if $\alpha \neq \gamma$, but is a nonzero vector if $\alpha = \gamma$. So the state $|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle$ has a component that lies along the vector $|\phi_{rest}^\gamma\rangle \otimes \left(\bigotimes_{k=1}^{2g} |\phi_{e'_k}^{[M_{\mathbf{B}}\gamma]_{k,\perp}} \right)$, but all of the other $|\phi_{rest}^\alpha\rangle \otimes |\phi_{\mathbf{B}}^\alpha\rangle$ are orthogonal to it. Thus $|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle$ cannot be written as a linear combination of the others, for each γ .

Now let $|\Phi\rangle = \sum_{j=1}^s |\chi_1^j\rangle |\chi_2^j\rangle \dots |\chi_{|E|}^j\rangle$ be any other expansion of $|\Phi\rangle$ into some number s of product states. Write it as

$$|\Phi\rangle = \sum_{j=1}^s |\chi_{E \setminus \mathbf{A}}^j\rangle \otimes |\chi_{\mathbf{A}}^j\rangle.$$

Then

$$\left(\bigotimes_{k=1}^{2g} \langle \phi_{e_k}^{[M_{\mathbf{A}}\gamma]_{k,\perp}} | \right) |\Phi\rangle = \sum_{j=1}^s \left(\left(\bigotimes_{k=1}^{2g} \langle \phi_{e_k}^{[M_{\mathbf{A}}\gamma]_{k,\perp}} | \right) |\chi_{\mathbf{A}}^j\rangle \right) |\chi_{E \setminus \mathbf{A}}^j\rangle.$$

Comparing this with Equation B2, we see that for each γ for which Ψ_γ is nonzero, $|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle$ can be written as a linear combination of the s states $|\chi_{E \setminus \mathbf{A}}^j\rangle$. Let D be the number of such nonzero Ψ_γ . Since each $|\phi_{rest}^\gamma\rangle \otimes |\phi_{\mathbf{B}}^\gamma\rangle$ is linearly independent, there must be enough states $|\chi_{E \setminus \mathbf{A}}^j\rangle$ to span a D dimensional space. So, $s \geq D$. Since this applies to any decomposition of the form $|\Phi\rangle = \sum_{j=1}^s |\chi_1^j\rangle |\chi_2^j\rangle \dots |\chi_{|E|}^j\rangle$, we conclude that $E_{Sch}(|\Phi\rangle) = \log_2 D$. \square

Appendix C: Proof of Theorem V.7

Specializing to punctured cylinder codes and the measurement ordering **LtoR** allows us to greatly simplify Equation 22. We consider two separate cases in turn.

1. Measurements between holes

We say that MBQC is “between” two holes when for some k , all of the edges in column $x_k + K_k$ are in the set

\tilde{E} , while all edges in column x_{k+1} are still in the set \hat{E} . In this subsection we will show that

Lemma C.1 *Theorem V.7 holds when computation is between holes.*

Proof With the encoding cocycles C'_k chosen as depicted in Figure 8, then the set A from Equation 22 contains all of the values from $2k + 1..2g$, and the set B is empty. Furthermore, C'_k lies entirely within the edge set \tilde{E} for $k \leq 2k$. Then Equation 22 becomes

$$p(|\phi_{\tilde{E}}\rangle) = \frac{1}{2^{|\partial\tilde{E}|-1}} \sum_{\gamma, \delta} c_\gamma c_\delta^* \prod_{j=2k+1}^{2g} \delta_{\gamma_j, \delta_j} \langle \phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^* | \bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta \sum_{u \in S} |K_{\tilde{E}}(u) \otimes K_{\tilde{E}}(u)\rangle. \quad (\text{C1})$$

In section V A, we saw that the state $\sum_{u \in S} |K_{\tilde{E}}(u) \otimes K_{\tilde{E}}(u)\rangle$ is the logical $+1$ X eigenstate $|\bar{+}\rangle$ associated with a surface code on the effective graph $G(\tilde{E}_1) \cup G(\tilde{E}_2)$. In this setting, graph $G(\tilde{E}_1) \cup G(\tilde{E}_2)$ has a natural embedding on a surface of genus $2k$, where the first k holes come from the subgraph $G(\tilde{E}_1)$ and the second k holes come from the subgraph $G(\tilde{E}_2)$. The set of $4k$ encoding cocycles for a surface code on $G(\tilde{E}_1) \cup G(\tilde{E}_2)$ can be chosen to be $C'_1 \dots C'_{2k}$ on the edges \tilde{E}_1 , along with $C'_1 \dots C'_{2k}$ on the edges \tilde{E}_2 . Then, the state

$$\bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta |K(G(\tilde{E}_1) \cup G(\tilde{E}_2))\rangle$$

is precisely the encoded X eigenstate $|X_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k}}\rangle$ in the surface-code space for $G(\tilde{E}_1) \cup G(\tilde{E}_2)$. If we furthermore define

$$\tilde{c}_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k}} := \sum_{\substack{\gamma_{2k+1} \dots \gamma_{2g} \\ \delta_{2k+1} \dots \delta_{2g} \\ \in \{0,1\}}} c_{\gamma_1 \dots \gamma_{2g}} c_{\delta_1 \dots \delta_{2g}}^* \prod_{j=2k+1}^{2g} \delta_{\gamma_j, \delta_j}, \quad (\text{C2})$$

then the probability of an outcome on the edges in \tilde{E} from the original graph is exactly proportional to an inner product with a state in the code space of the surface code on $G(\tilde{E}_1) \cup G(\tilde{E}_2)$:

$$p(|\phi_{\tilde{E}}\rangle) = \frac{1}{\sqrt{2^{|\partial\tilde{E}|-1}}} \langle \phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^* | \sum_{\substack{\gamma_1 \dots \gamma_{2k} \\ \delta_1 \dots \delta_{2k}}} \tilde{c}_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k}} |X_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k}}^{G'(\tilde{E})}\rangle. \quad (\text{C3})$$

Here \tilde{c} is an effective tensor of coefficients in the encoded X-basis for a state in the surface-code space of $G'(\tilde{E}) := G(\tilde{E}_1) \cup G(\tilde{E}_2)$. The inner product between this state and the product state $|\phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^*\rangle$ yields the partial

measurement probability. This confirms Theorem V.7 for the cases when computation is between holes. Now, we turn to the other stages of MBQC on a punctured cylinder code state.

2. Measurements crossing holes

If the boundary $\partial\tilde{E}$ contains vertices in a column between x_k and $x_k + K_k$ for any k , then some acrobatics are required to keep Equation 22 expressible in the simple form of Equation C1. This scenario occurs as the computation “crosses holes” from left to right on the lattice G . Figure 11 below shows the part of a punctured cylinder graph G around the k^{th} hole. In particular, we will focus on the measurement steps after edge a in Figure 11 has been measured, but before edge b is measured. Before edge a is measured, or after edge b is measured, the situation is no more complicated than when computation is “between holes”. In this subsection we will show that nevertheless,

Lemma C.2 *Theorem V.7 holds when computation is crossing holes.*

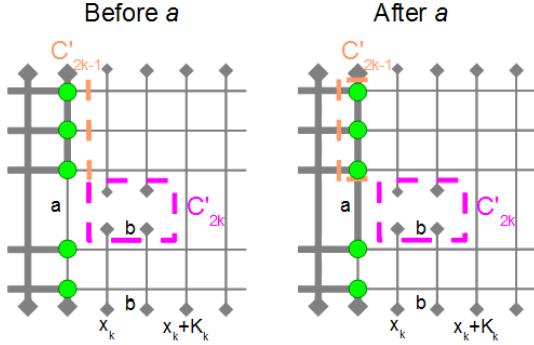


FIG. 11: (Color online) The part of a punctured cylinder graph around the k^{th} hole. Two stages are depicted, just before and just after the edge a is measured. The set \tilde{E} is shown in bold, and the vertices in $\partial\tilde{E}$ are marked by circles (green). A choice of the non-trivial cocycles C'_{2k-1} and C'_{2k} that are convenient for each step are shown as dotted lines (orange and purple, respectively).

Proof On the left side of Figure 11, we show the relevant encoding cocycles C'_{2k-1} and C'_{2k} , chosen in accordance with Figure 8. From this and the **LtoR** ordering, it is clear that as soon as the edge a is measured, the set B is no longer empty. Rather, $B = \{2k-1\}$ i.e., there exists no $\hat{x} \in E_0(\tilde{E})$ such that $|\hat{x} \cap C'_{2k-1}| = 1$, yet $C'_{2k-1} \cap \tilde{E} \neq \emptyset$. This is because there is no cycle that can “wrap around” the k^{th} hole without using the edge a or one to its left. With $B \neq \emptyset$, Equation 22 becomes more complicated. However, we can avoid this by considering the alternative encoding cocycle C'_{2k-1} depicted on the

right side of Figure 11 as soon as the edge a is measured. This cocycle is homologous to the first (they differ only by the bitwise addition of δ_v for a set of vertices v) and hence their effect on the surface-code space is identical.

With C'_{2k-1} chosen in this way, we have $A = \{2k \dots 2g\}$ and $B = \emptyset$. Furthermore, $C'_j \in \tilde{E}$ for all $j = 1 \dots 2k-1$. Equation 22 takes the form, like Equation C1

$$p(|\phi_{\tilde{E}}\rangle) = \frac{1}{\sqrt{2^{|\partial\tilde{E}|-1}}} \sum_{\gamma, \delta} c_{\gamma} c_{\delta}^* \prod_{j=2k}^{2g} \delta_{\gamma_j, \delta_j} \langle \phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^* | \bar{Z}_{\tilde{E}_1}^{\gamma} \bar{Z}_{\tilde{E}_2}^{\delta} | K(G(\tilde{E}_1) \cup G(\tilde{E}_2)) \rangle. \quad (C4)$$

What remains now is to define a natural embedding of the graph $G(\tilde{E}_1) \cap G(\tilde{E}_2)$, which requires a more complicated topology than in the case of measurements between holes. To aid in this, we will employ two graph manipulations that only affect the overlap between $|K(G)\rangle$ and a product state up to a constant of proportionality. For any connected graph G , we may perform the following operations:

- **Edge addition:** We may add an edge e to G , then measure the qubit associated with the added edge to be in the $|0\rangle$ state. The edge can be added between existing vertices on G , or by adding a new vertex and connecting it to G with the new edge. Call the new graph obtained after edge addition G' . Then: $\langle 0_e | K(G') \rangle = \frac{1}{\sqrt{2}} |K(G)\rangle$.
- **Vertex splitting:** We can split any vertex into two, and add an edge e in between the two resultant vertices. The edges incident on the vertex that is split can be divided arbitrarily between the two resultant vertices. Then measure the new qubit to be in the $|+\rangle$ state. Call the new graph obtained by vertex splitting G' . Then: $\langle +_e | K(G') \rangle = \frac{1}{\sqrt{2}} |K(G)\rangle$

Using edge addition and vertex splitting [37], we transform the graph $G(\tilde{E}_1) \cap G(\tilde{E}_2)$ into an effective graph $G'(\tilde{E})$ that has a natural embedding on a surface of genus $2k-1$. An example of this is shown in Figure 12.

A surface code on $G'(\tilde{E})$ encodes $4k-2$ qubits. The encoding cocycles $\bar{C}'_1 \dots \bar{C}'_{4k-2}$ on the embedded graph $G'(\tilde{E})$ can be chosen as follows: let the first $2k-2$ cocycles be $\bar{C}'_j := C'_j$ applied to the edges \tilde{E}_1 , and the last $2k-2$ cocycles be $\bar{C}'_{j+2k} := C'_j$ applied to the edges \tilde{E}_2 . The cocycle for qubit numbered $2k-1$ can be chosen as the cocycle $\bar{C}'_{2k-1} := C'_{2k-1}$ applied to the edge set \tilde{E}_1 . Finally the cocycle \bar{C}'_{2k} for qubit $2k$ belongs to the newly added edges, as depicted in Figure 12.

Let \tilde{E} denote the edges which are added to $G_1(\tilde{E}) \cup G_2(\tilde{E})$ to construct $G'(\tilde{E})$, and let $|\bar{\phi}_{\tilde{E}}\rangle$ denote a tensor product of the $|+\rangle$ state for each of the horizontal edges (added by vertex splitting), and $|0\rangle$ for each of the vertical

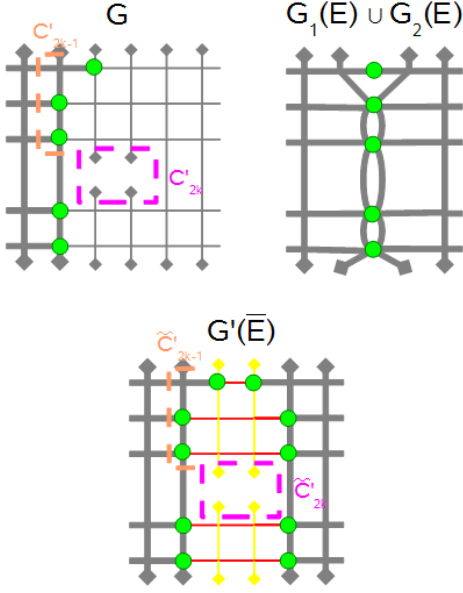


FIG. 12: (Color online) The graphs G , $G(\tilde{E}_1) \cap G(\tilde{E}_2)$, and $G'(\tilde{E})$ for a “crossing hole” step of MBQC. The vertical nonbold edges of $G'(\tilde{E})$ (yellow) are measured in the $|0\rangle$ state, while the horizontal nonbold edges (red) are measured in the $|+\rangle$ state. Encoding cocycles are shown for G and $G'(\tilde{E})$.

edges (added by edge addition). We can recast Equation C4 as

$$p(|\phi_{\tilde{E}}\rangle) = \frac{1}{\sqrt{2^{|\partial\tilde{E}|-|\tilde{E}|-1}}} \sum_{\gamma,\delta} c_\gamma c_\delta^* \prod_{j=2k}^{2g} \delta_{\gamma_j, \delta_j} \langle \phi_{\tilde{E}} \otimes \bar{\phi} \otimes \phi_{\tilde{E}}^* | \bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta | K(G'(\tilde{E})) \rangle, \quad (\text{C5})$$

where we can take $\bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta$ to be

$$\prod_{e \in \tilde{C}'_{2k-1}} Z_e^{(\gamma \oplus \delta)_{2k-1}} \prod_{j=1}^{2k-2} \left(\prod_{e \in \tilde{C}'_j} Z_e^{\gamma_j} \prod_{e \in \tilde{C}'_{j+2k}} Z_e^{\delta_j} \right)$$

which depends only on the bitwise sum $(\gamma \oplus \delta)_{2k-1}$ because the cocycle C'_{2k-1} applied to the edge set \tilde{E}_2 is homologous to \tilde{C}'_{2k-1} on the graph $G'(\tilde{E})$. So, if both γ_{2k-1} and δ_{2k-1} are equal to one, there is no overall effect on the state $|K(G'(\tilde{E}))\rangle$.

Now, since all of the edges in the set \tilde{C}'_{2k} are measured in the state $|0\rangle$, we may insert the operator $\bar{Z}_{2k} := \prod_{e \in \tilde{C}'_{2k}} Z_e^{\gamma_{2k}}$ with impunity. Then

$$\bar{Z}_{\tilde{E}_1}^\gamma \bar{Z}_{\tilde{E}_2}^\delta \prod_{e \in \tilde{C}'_{2k}} Z_e^{\gamma_{2k}} |K(G'(\tilde{E}))\rangle$$

is precisely the encoded X eigenstate

$$|X^{G'(\tilde{E})}_{\gamma_1 \dots \gamma_{2k-2}, (\gamma \oplus \delta)_{2k-1}, \gamma_{2k}, \delta_1 \dots \delta_{2k-2}}\rangle$$

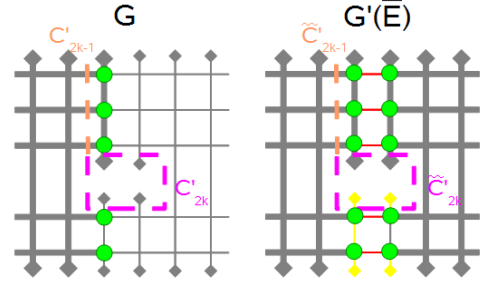


FIG. 13: (Color online) The graphs G and $G'(\tilde{E})$ during a stage of MBQC where C'_{2k} is split across \tilde{E} and \hat{E} .

in the surface-code space of $G'(\tilde{E})$. If we now define

$$\tilde{c}_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k-2}} := \sum_{\substack{\gamma_{2k+1} \dots \gamma_{2g} \\ \delta_{2k-1} \dots \delta_{2g}}} c_{\gamma_1 \dots \gamma_{2k-2}, (\gamma \oplus \delta)_{2k-1}, \gamma_{2k} \dots \gamma_{2g}} c_{\delta_1 \dots \delta_{2g}}^* \prod_{j=2k}^{2g} \delta_{\gamma_j, \delta_j}, \quad (\text{C6})$$

then the probability of a outcome on the edges in \tilde{E} from the original graph is exactly proportional to an inner product with a state in the code space of the surface code on $G'(\tilde{E})$:

$$p(|\phi_{\tilde{E}}\rangle) = \frac{1}{\sqrt{2^{|\partial\tilde{E}|-1}}} \langle \phi_{\tilde{E}} \otimes \phi_{\tilde{E}}^* | \sum_{\substack{\gamma_1 \dots \gamma_{2k} \\ \delta_1 \dots \delta_{2k-2}}} \tilde{c}_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k-2}} |X^{G'(\tilde{E})}_{\gamma_1 \dots \gamma_{2k}, \delta_1 \dots \delta_{2k-2}}\rangle, \quad (\text{C7})$$

which again takes the form of the inner product between a surface-code state and product state. One can find a suitable $G'(\tilde{E})$ to put $p(|\phi_{\tilde{E}}\rangle)$ into the form of Equation C7 at all MBQC stages while crossing a hole; we have shown just one example of such a stage. During later stages the encoding cocycle C'_{2k} will be split across the measured and unmeasured edges: $C'_{2k} \cap \tilde{E} \neq \emptyset$ and $C'_{2k} \cap \hat{E} \neq \emptyset$. However, we can always still “complete” the partial cocycle $C'_{2k} \cap \tilde{E}$ from G to a cocycle \tilde{C}'_{2k} on $G'(\tilde{E})$ by adding edges from \tilde{E} that are measured in the $|0\rangle$ state. An example of this is shown in Figure 13. Note that given our ordering of measurements, there still exists an $\hat{x} \in E_0(\hat{E})$ such that $|\hat{x} \cap C'_{2k}| = 1$ until the edge b from Figure 11 is measured. Yet, once b is measured $C'_{2k} \in \tilde{E}$, so $2k \notin B$ and Equation C7 holds for all stages. This completes the proof of Theorem V.7 for all stages of computation.

Appendix D: MBQC with the states $|\bar{C}^{\alpha, \beta}\rangle$

With Theorem V.7, we have reduced the problem of simulating MBQC on punctured cylinder code states

with **LtoR** to the evaluation of an inner product

$$\langle \phi(G'(\tilde{E})) | \left(\sum_{\gamma \in \{0,1\}^{\otimes 2g'}} \tilde{c}_\gamma |X_\gamma^{G'(\tilde{E})}\rangle \right), \quad (\text{D1})$$

where $G'(\tilde{E})$ is an effective lattice of genus $g' = 2k$ or $2k - 1$, k is the number of holes in the set of qubits that have already been measured, and $|\phi(G'(\tilde{E}))\rangle$ is a product state. Recall that in the associated encoded X-eigenbasis (corresponding to a canonical polygonal schema), the state $|\bar{C}^{\alpha,\beta}\rangle$ has coefficients

$$c_{\gamma,\rho} := \frac{1}{2^g} \prod_{j=1}^g (-1)^{\alpha_j \beta_j + (\alpha \oplus \gamma)_j (\beta \oplus \rho)_j},$$

where the notation $c_{\gamma,\rho}$ separates the odd and even numbered encoded qubits into two g -component bitstrings γ and ρ . Here we will show that for MBQC with punctured cylinder code states $|\bar{C}^{\alpha,\beta}\rangle$, the tensor $\tilde{c}_{\gamma,\rho}$ takes this same form, and thus the state

$$\sum_{\gamma,\rho \in \{0,1\}^{\otimes g'}} \tilde{c}_{\gamma,\rho} |X_{\gamma,\rho}^{G'(\tilde{E})}\rangle$$

in Equation D1 can be interpreted as a state $|\bar{C}^{\alpha',\beta'}\rangle$ in the code space of the surface code on the effective graph $G'(\tilde{E})$, for some $\alpha', \beta' \in \{0,1\}^{\otimes g'}$. Then the efficiency of sampling follows by Equation 11. Here the notation associates γ with the even numbered qubits and ρ with the odd: e.g. $\tilde{c}_{\gamma,\rho} := \tilde{c}_{\gamma_1,\rho_1,\gamma_2,\rho_2,\dots,\rho_{g'}}$ (note the possible confusion with Equations C3 and C4).

To verify the above claim, we begin with the case where computation is between holes. Using the definition of the \tilde{c} coefficients (Equation C2), after the summation $\tilde{c}_{\gamma_1 \dots \gamma_k \delta_1 \dots \delta_k, \rho_1 \dots \rho_k \epsilon_1 \dots \epsilon_k}$ works out to be:

$$\frac{1}{2^{2k}} \prod_{j=1}^k (-1)^{\alpha_j \beta_j + (\alpha \oplus \gamma)_j (\beta \oplus \rho)_j} (-1)^{\alpha_j \beta_j + (\alpha \oplus \delta)_j (\beta \oplus \epsilon)_j}.$$

This is exactly the tensor of coefficients for the state $|\bar{C}^{\alpha',\beta'}\rangle$ in the code space of a punctured cylinder code with $2k$ slots, labelled by bitstrings that are symmetric between the first and last k entries: $\alpha' := \alpha \& \alpha, \beta' := \beta \& \beta$, where $\&$ denotes concatenation. The encoded Z cocycles are again those of a canonical encoding scheme, so local overlaps with $|\bar{C}^{\alpha',\beta'}\rangle$ can be computed efficiently in $|E|$ and g .

When crossing holes, we perform the summation of Equation C6 for $\tilde{c}_{\gamma_1 \dots \gamma_k \delta_1 \dots \delta_{k-1}, \rho_1 \dots \rho_k \epsilon_1 \dots \epsilon_{k-1}}$ to obtain:

$$\begin{aligned} & \frac{1}{2^{2k}} \prod_{j=1}^{k-1} (-1)^{(\alpha \oplus \gamma)_j (\beta \oplus \rho)_j} (-1)^{(\alpha \oplus \delta)_j (\beta \oplus \epsilon)_j} \\ & \sum_{\delta_k \in \{0,1\}} (-1)^{(\alpha \oplus \gamma \oplus \delta)_k (\beta \oplus \rho)_k} (-1)^{(\alpha \oplus \delta)_k (\beta \oplus \rho)_k} \\ & = \frac{1}{2^{2k-1}} \prod_{j=1}^{k-1} (-1)^{(\alpha \oplus \gamma)_j (\beta \oplus \rho)_j} (-1)^{(\alpha \oplus \delta)_j (\beta \oplus \epsilon)_j} \\ & \quad (-1)^{\gamma_k (\beta \oplus \rho)_k}, \end{aligned}$$

which is again the tensor describing $|\bar{C}^{\alpha',\beta'}\rangle$ in the code space of the surface code for $G'(\tilde{E})$, where $\alpha' := \alpha_1, \dots, \alpha_{k-1}, 0, \alpha_1, \dots, \alpha_{k-1}$ and $\beta' := \beta_1, \dots, \beta_k, \beta_1, \dots, \beta_{k-1}$. \square

-
- [1] D. Gottesman (Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, 1999).
 - [2] R. Jozsa and A. Miyake, Proceedings of the Royal Society A **464** (2008).
 - [3] L. G. Valiant (Proceedings of the 33rd Annual ACM Symposium on the Theory of Computation (STOC01), 2001).
 - [4] B. M. Terhal and D. P. DiVincenzo, Physical Review A **65**, 032325 (2002).
 - [5] G. Vidal, Physical Review Letters **91**, 147902 (2003).
 - [6] R. Jozsa and N. Linden, Proceedings of the Royal Society of London A **459**.
 - [7] I. Markov and Y. Shi., SIAM Journal on Computing **38**, 963 (2008).
 - [8] M. V. den Nest, W. Dur, G. Vidal, and H. J. Briegel, Physical Review A **75**, 012337 (2007).
 - [9] M. V. den Nest, arXiv:1204.3107 (2012).
 - [10] D. Gross, S. T. Flammia, and J. Eisert, Physical Review Letters **102**, 190501 (2009).
 - [11] M. J. Bremner, C. Mora, and A. Winter, Physical Review Letters **102**, 190502 (2009).
 - [12] A. Y. Kitaev, Annals of Physics **303**, 2 (2003).
 - [13] E. Dennis, A. Y. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
 - [14] M. V. den Nest, W. Dur, and H. J. Briegel, Physical Review Letters **98**, 117207 (2007).
 - [15] S. Bravyi and R. Raussendorf, Physical Review A **76**, 022304 (2007).
 - [16] S. Bravyi, in *Proceedings of the Royal Society A Mathematical Physical and Engineering Sciences* (2008).
 - [17] A. Galluccio, M. Loebl, and J. Vondrák, Physical Review Letters **84**, 5924 (2000).
 - [18] B. Mohar and C. Thomassen, *Graphs on Surfaces* (Johns Hopkins University Press, Baltimore, 2001).
 - [19] Here we use X Pauli operators for the faces and Z for the vertices (as in [15]), rather than Z operators for the faces and X for the vertices as in most treatments of the surface code. This choice simplifies our discussion. The two code spaces are equivalent up to a global Hadamard transformation.
 - [20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 1st ed. (Cambridge University Press, 2000).
 - [21] Note that some authors require a cycle to be non-null and connected, or contain a maximum of two edges inci-

- dent on any vertex. Our definition of cycle also called a *Eulerian subgraph*.
- [22] D. Eppstein (SODA '03 Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms, 2003).
 - [23] S. Cabello and B. Mohar, *Discrete and Computational Geometry* **37**, 213 (2007).
 - [24] In [38] a distinction is made between ‘strong’ simulations in which certain quantities are computed exactly, and ‘weak’ simulations in which approximations to those quantities are obtained through sampling. In this terminology, the first of the above simulations is a special case of a ‘strong’ simulation and the second simulation is ‘weak’, which may seem counterintuitive after the above. While the second notion of simulation is a weaker in terms of accuracy, it can at least sufficiently closely approximate a wider variety of quantities of interest.
 - [25] P. Kasteleyn, in *Graph Theory and Theoretical Physics* (1967) pp. 43–110.
 - [26] M. E. Fisher, *Journal of Mathematical Physics* **7**, 1776 (1966).
 - [27] D. Browne, E. Kashefi, M. Mhalla, and S. Perdrix, *New J. Phys.* **9**, 250 (2007).
 - [28] R. Raussendorf and H. J. Briegel, *Physical Review Letters* **86**, 5188 (2001).
 - [29] C. M. V. Vliet, *Equilibrium and non-equilibrium statistical mechanics* (World Scientific, Singapore, 2008).
 - [30] L. Goff, MSc Thesis: University of British Columbia (2011).
 - [31] J. Eisert and H. J. Briegel, *Physical Review A* **64**, 022306 (2001).
 - [32] A. Galluccio and M. Loeb, *The Electronic Journal of Combinatorics* **6**, R6 (1999).
 - [33] F. Barahona, *Journal of Mathematical Physics* **15**, 3241 (1982).
 - [34] J. Stillwell, *Classical Topology and Combinatorial Group Theory* (Springer-Verlag, New York, 1980).
 - [35] S. Cabello and B. Mohar, in *13th Annual European Symposium on Algorithms* (2005).
 - [36] P. Kasteleyn, *Physica* **27**, 1209 (1961).
 - [37] We note that the edge addition and vertex splitting are exactly the opposite of the *graph minor* operations: edge contraction, edge deletion, and deletion of isolated vertices. This implies that the class of graphs under consideration is *minor closed*. In principle, this means that our considerations on the punctured cylinder graphs are applicable to any graph, because the family of all punctured cylinder graphs contains every graph as a minor. This follows from a result by Robertson and Seymour [39] to the effect that for any two graphs G and H that can be embedded on a surface S of genus $g \geq 1$, H is a minor of G if the face-width of G is at least $k(H)$, where $k(H)$ is an integer that depends on the graph H . Face-width is the minimum number of edges of a graph that any non-contractible loop on S must cross, which is a controllable parameter within the family of punctured cylinder graphs. However, this result is not of practical use here without knowledge of how $k(H)$ scales with the size and genus of H .
 - [38] M. V. den Nest, *Quantum Information & Computation* **10**, 3 (2010).
 - [39] N. Robertson and P. Seymour, *Journal of Combinatorial Theory, Series B.* **45**, 244 (1988).